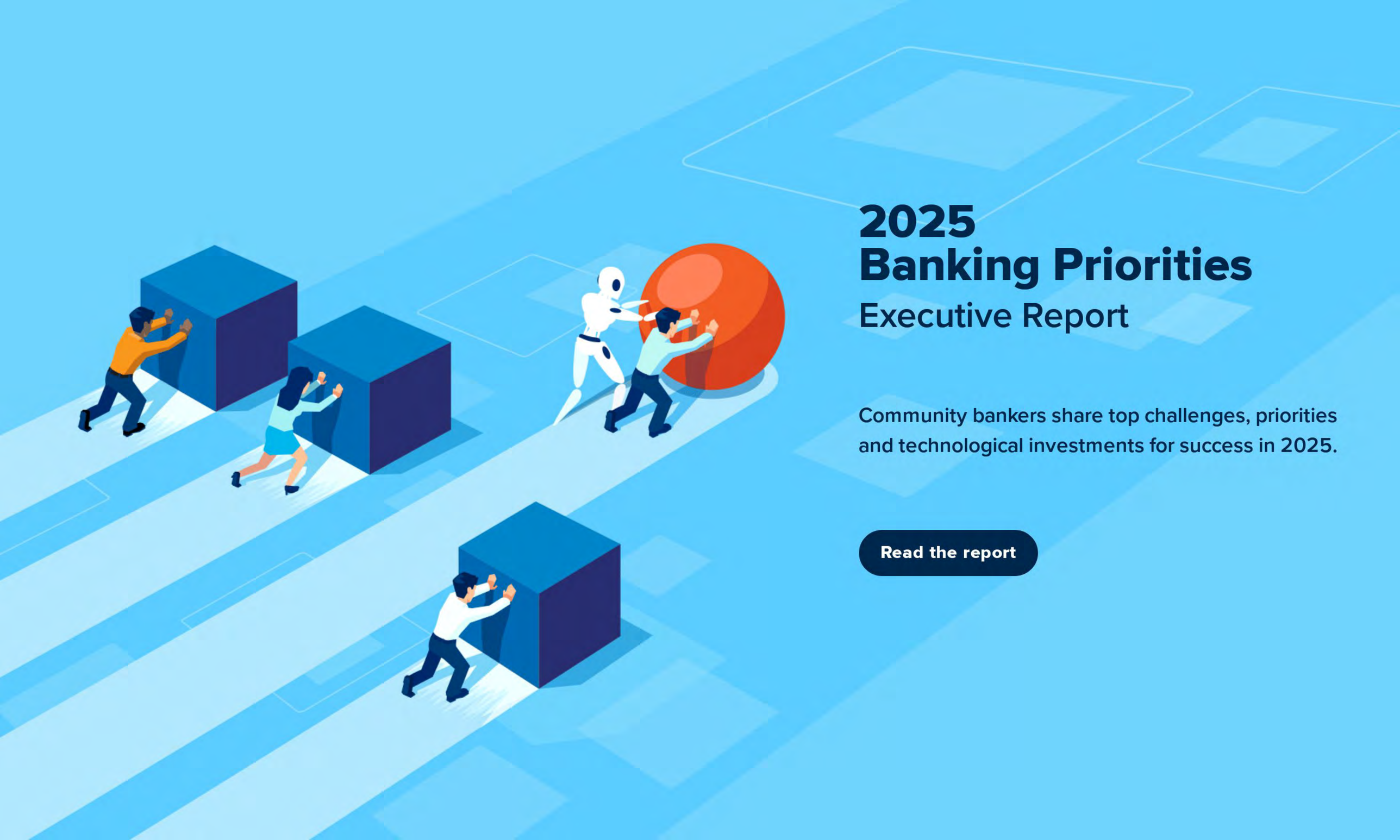


2025 Banking Priorities

Executive Report

Community bankers share top challenges, priorities and technological investments for success in 2025.

Read the report

Contents

Introduction to the 2025 Report 3
Taking the Pulse of Community Banks 4
Key Highlights and Preview 5
Top Issues on Bankers' Minds 6
Key Technology Trends in 2025 7
Bankers' Strategic Priorities 8
Embracing a Modern Core 9
Artificial Intelligence (AI) 10
Top Technology Investments 11
Cybersecurity 12
Fraud 13
Regulatory Issues 14
Conclusion 15
Appendix 16
Resources 18
Download the PDF 19

Bankers Look Ahead to 2025

Community Bankers Embrace an Era of AI and Increased Efficiency

AI has emerged as a transformative force in the financial services industry. From streamlining internal processes to fighting cybersecurity and financial crime threats, banks are exploring AI and the opportunities it creates while keeping in mind inherent risks.

In addition to expressing interest in expanding AI use, bankers' responses to the 2025 Banking Priorities survey indicate continued optimism and commitment to modernization. Bankers share their top challenges, strategies and technology investments as they plan for 2025. While strategies vary depending on individual institutions, increasing efficiencies also arose as a recurring theme as banks strive to remain competitive and meet evolving customer expectations in a digital-first world.

Facing rapid technological change and shifting consumer preferences, banks are doubling down on reducing manual processes and taking advantage of efficiencies created by automation. Continued adoption of open banking, enhanced cybersecurity and evolving regulatory concerns broaden the areas of focus financial institutions must consider when developing their strategies. But these areas also represent a tremendous opportunity for those that adapt.

About CSI's 2025 Banking Priorities Survey

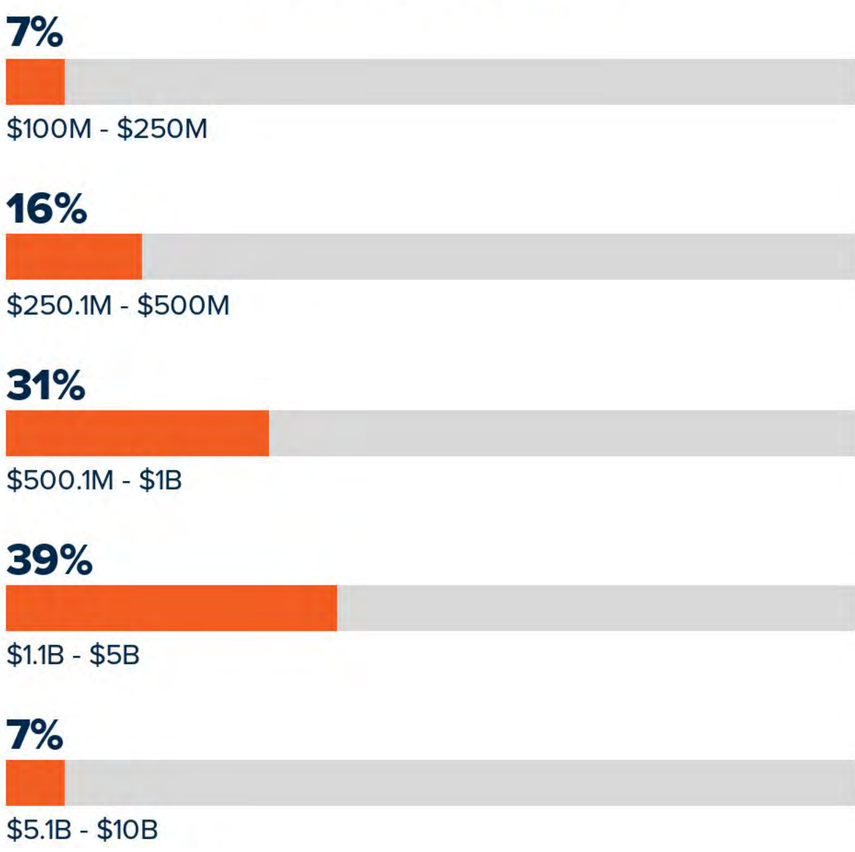
Navigating the twists and turns of the banking landscape takes foresight, flexibility and a clear strategy—that's why CSI conducts an annual survey of community financial institutions nationwide to understand their perspective for the year ahead. We explore their strategic priorities, market share strategies, upcoming technological investments and more.

We understand the complex challenges facing community banks and want to provide a look into the industry to help institutions identify trends and solutions used by other institutions while providing data to benchmark their own performance. This annual research initiative sheds light on bankers' approaches to staying competitive and offers expert guidance around those plans.

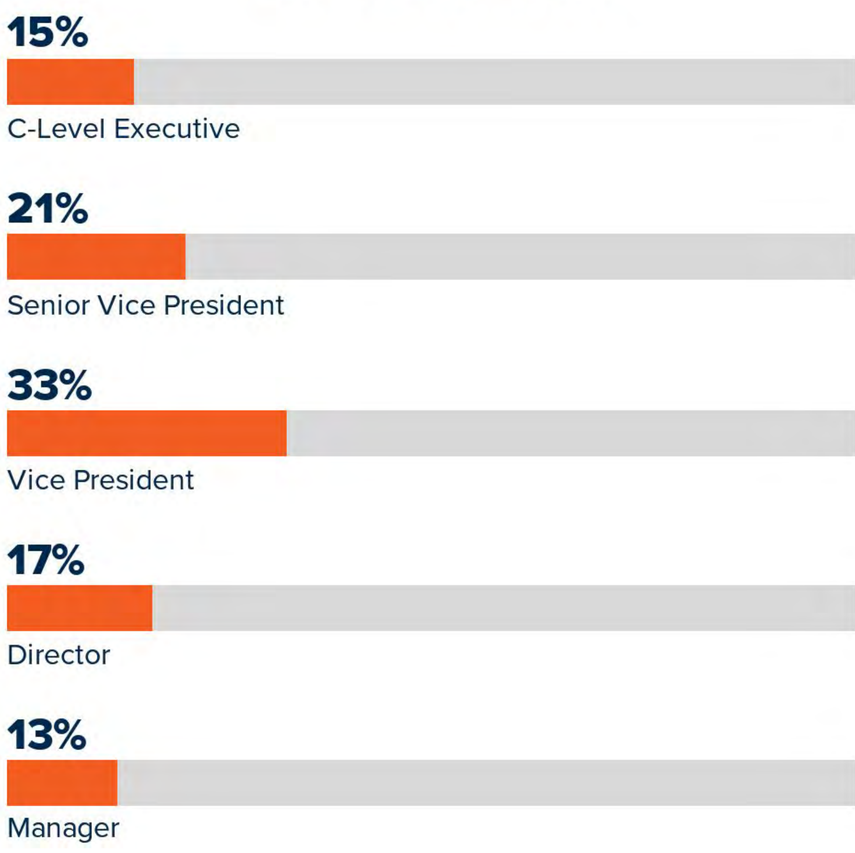
Let this report serve as a guide to facing the challenges in 2025 head on, turning them into opportunities to meet and exceed customer expectations.

Independent research firm CITE Research administered the tenth iteration of the survey, distributing it to community bankers across the United States throughout October 2024. 250 bankers at manager level or above responded, strategically dispersed across these demographics:

Institution Asset Size



Role of Respondent



Explore our interactive report to uncover their responses, as well as analyses and insight from industry experts. All percentages are rounded to the nearest whole percentage point with an estimated margin of error of just slightly over 6%.

Taking the Pulse of Community Banks

Community banks, often defined as locally operated institutions with under $10 billion in assets, support local economies and cultivate personal relationships with their customers. Their commitment to relationship-based banking and community involvement inspires trust and loyalty, making them valuable partners in regional economic stability and growth. This report sheds light on their strategies and priorities to maintain and expand influence within their communities.

The Banking Landscape Going into 2025

Bankers navigated economic pressures, evolving cyber threats, increasing regulatory requirements and demand for continued personalized, customer-centric services throughout 2024.

Bankers' responses to the statements below provide a snapshot of their perspectives on the industry.

Confidence in Community Banking

While bankers face evolving industry challenges, an overwhelming majority expressed strong optimism about the future of community banking. Only 8% held a less than optimistic view.

I'm optimistic about the future of community banking.

50%
Strongly Agree

41%
Somewhat Agree

8%
Somewhat Disagree

Growth and Engagement

Growth remains a priority for banks, as a majority seek to expand and increase deposits. 91% strongly or somewhat agree their customers are engaged on digital channels, reflecting consumers' preference for digital engagement. Only 9% feel they aren't growing their customer base.

My bank's customers are engaged on digital channels.

53%
Strongly Agree

38%
Somewhat Agree

7%
Somewhat Disagree

My bank is growing its existing customer base.

43%
Strongly Agree

48%
Somewhat Agree

9%
Somewhat Disagree

My bank is focused on increasing deposits.

44%
Strongly Agree

47%
Somewhat Agree

7%
Somewhat Disagree

Technology and Efficiencies

An institution's growth and engagement depend partly on efficient processes and modern technology. An overwhelming 95% of respondents agree that they are enabling choice for customers through the latest technology. However, over 40% strongly agree their processes could be more efficient.

My bank's processes could be more efficient.

42%
Strongly Agree

47%
Somewhat Agree

9%
Somewhat Disagree

My bank is enabling choice for our customers through the latest technology.

49%
Strongly Agree

46%
Somewhat Agree

5%
Somewhat Disagree

The Future of Branches

86% of respondents believe the branch will remain relevant for at least the next 10 years, slightly down from 92% last year. This prediction suggests plans to meet customers in the channel of their choice with a blend of digital innovation, traditional customer engagement and innovative in-branch experiences.

The branch will remain relevant for the next 10 years.

43%
Strongly Agree

43%
Somewhat Agree

11%
Somewhat Disagree

2025 Banking Priorities
Contents

See the Survey Responses
Appendix

Key Highlights and Preview

The 2025 survey revealed distinct challenges and opportunities that face community bankers. Noteworthy highlights of the following pages include:

Cybersecurity and Data Privacy

Looking into 2025, community financial professionals believe cybersecurity/data privacy will affect the industry most.

- 28% listed cybersecurity/data privacy as the issue most likely to affect the industry in 2025.
- To combat these increasing threats, banks are deploying various approaches like risk assessments and other cybersecurity tools.

$6.08M

The average cost of a data breach in the financial industry rose from $5.9 million in 2023 to $6.08 million in 2024.

Source: Cost of a Data Breach Report 2024[1]

Banks Embrace Core Modernization

Almost all bankers surveyed identified planned strategies to modernize their core banking system, moving away from outdated legacy applications.

- 62% of banks plan to invest in core or ancillary products that support ongoing innovation in 2025.
- Moreover, 57% of bankers are using or planning to expand use of integrated solutions supported by open APIs while 53% plan to evaluate technology in terms of its ability to support open banking.

$330B

It's estimated that total open banking transactions will reach $330 billion in 2027, having reached $57 billion in 2023.

Source: Juniper[2]

Efficiency Tops List of Strategic Priorities

Increasing operational efficiencies emerged as a leading area of focus for bankers, with 44% selecting this as a top strategic priority.

- 40% of bankers selected deposit growth as one of their top three priorities, signaling banks' focus on capturing new accounts.
- However, only 22% of community banks plan to focus on loan growth as a strategic priority.

$100K in Savings

A recent survey revealed 52% of banking executives reported saving at least $100,000 annually because of automation, and respondents cited increased efficiencies among top goals.

Source: The Financial Brand[3]

Artificial Intelligence (AI) Remains Major Tech Trend

For the second year in a row, bankers chose AI as the top technology trend most likely to affect the financial industry in 2025.

- 33% chose AI as the top trend to watch for 2025, suggesting banks are evaluating its benefits and beneficial use cases.
- Most are interested in using AI for fraud and AML detection and prevention (91%) or customer service (90%), and eight in 10 bankers expressed concern about the technology.

21% net increase

As a driver of economic growth, AI is expected to contribute a 21% net increase to the U.S. GDP by 2030.

Source: Forbes[4]

Top Issues on Bankers' Minds

We asked community bankers to identify the issue most likely to affect the financial industry in 2025. Their responses offer insight into how they perceive the environment and the range of pressures they face heading into the new year.

What Did Bankers Identify as Top Issues for 2025?

In anticipating the most impactful industry issues, financial professionals identified the following key concerns.

Cybersecurity/Data Privacy

28%

28% of bankers selected this as the top concern for the upcoming year. From phishing and ransomware to account takeover and cloud attacks, cyber threats are constantly evolving as motivated bad actors use the latest tactics.

Interest Rates

19%

Coming second, 19% of bankers view interest rates as the most pressing concern for 2025. Bankers' concern for interest rates has lowered since 2023, potentially due to stabilized rates and anticipated future rate changes from the Fed.

Regulatory Change

14%

Ranking third, regulatory change was identified by 14% of respondents as the most pressing issue. This is an increase from the 8% reported last year, showing bankers are taking note of an evolving regulatory landscape.

"Banks need to stay on top of security, and the landscape is changing on a daily basis. Security needs to be highly prioritized by the bank and consumers."

Source: Survey Participant

The remaining options each took less than 12% of the vote.

The 2024 Election

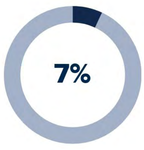
Nearly one in 10 bankers selected the 2024 election as the most impactful issue. Since this survey was conducted in the month prior to the general election, bankers could've been considering any potential legislative or regulatory implications from an administration change.

Recruiting and Retaining Employees

Only 11% of bankers selected talent acquisition and retention, the same percentage as last year's survey. This overall optimism could mean bankers perceive the job market as relatively stable.

Mergers and Acquisitions

10% of bankers believe mergers and acquisitions to be the top issue.



Fraud

Less than 10% of respondents selected fraud, which is quite the contrast to last year when fraud took 30% of the vote. The drop from last year likely stems from a heightened focus on other issues at the time of response.

Key Technology Trends in 2025

Financial institutions must keep an eye on the technology landscape to remain competitive. Aside from the top standout, bankers generally agreed on the key technological trends:

Artificial Intelligence (AI)

33%

For the second year, AI was named as the most impactful technology trend, with 33% of respondents recognizing its transformative potential. This endorsement follows years of headlines around AI's potential to revolutionize risk management, customer service and more.

Real-time Fraud Detection

17%

As fraud continues to skyrocket, 17% of bankers selected real-time fraud detection as the top technology trend poised to affect the industry in 2025.

Banking as a Service (BaaS)

17%

BaaS emerged as another impactful trend, capturing 17% of respondents' votes. This trend allows collaboration between financial institutions, fintechs and neobanks to champion innovation.

Digital Transformation

16%

Digital transformation followed closely at 16%, highlighting the focus on digital channels for streamlined processes and delivering elevated customer experiences.

APIs/Open Banking

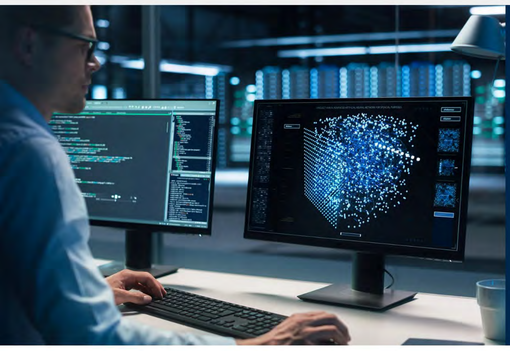
11%

APIs and open banking garnered 11% of the vote, a slight increase from last year's results at 7%. Open banking through APIs provides potential for every bank, from automated workflows to integrated platforms.

Instant Payments

6%

The Fed's instant payments network launched in 2023, leading instant payments to receive 6% of the vote.



Industry Insight

The trends above reflect a rapidly changing financial landscape, where technology shapes how banks operate. AI is driving the industry conversation as banks explore the advantages and risks of this technology, including related solutions like real-time fraud detection.

BaaS continues to garner bankers' interest, though slightly less than the 20% reported last year. A BaaS model involves nonbank companies offering financial services by partnering with a financial institution and utilizing its regulated banking infrastructure. Built on the foundations of an open banking framework, BaaS uses APIs to access banking functionality. However, banks should understand the regulatory environment and requirements when evaluating a BaaS partnership.

Most banks are well on their way to some type of digital transformation, having implemented digital banking and online account opening. Banks should avoid becoming stagnant in this process and continue improving the user experience on digital channels.

Expert Perspective

For many banks, AI represents an area of heightened focus and buzz, but many are still in the process of understanding how to manage AI in a regulated industry. AI engines are becoming more popular to boost business functions, but banks must understand how their data will be used to avoid unintentional disclosure.

As AI unlocks opportunities for fraudsters by making it easier to execute social engineering attacks, it's no surprise bankers identified real-time fraud detection as a top trend. From synthetic identity fraud to check fraud, AI-powered solutions that analyze copious amounts of data stand to help institutions fight back against these evolving threats.

Although only 11% identified open banking/APIs as a top trend, institutions who embrace open banking and provide their customers with best-of-breed products and services will be better positioned to navigate the competitive banking landscape.

"We hope to use AI technology to further enhance risk prevention capabilities and business security levels."

Source: Survey Participant

Bankers' Strategic Priorities

Strategic priorities help community financial institutions focus on areas to drive value, providing a roadmap for achieving long-term goals.

When asked about their strategic priorities for 2025, increasing operational efficiencies topped the list. Banks with asset sizes of $500M - $5B were most likely to select this priority. Deposit growth and technology modernization rounded out the top three, demonstrating bankers' focus on expanding their accounts and updating technology to meet customer expectations and deliver enhanced functionality.

44%

Increasing Operational Efficiencies

40%

Deposit Growth

38%

Technology Modernization

While the top three strategic priorities stand out, the survey also reveals other areas of focus following closely behind:

37%

Strengthening Cybersecurity

31%

Opening New Branches

30%

Market Expansion

30%

Mergers and Acquisitions

28%

Customer Support

22%

Loan Growth

Industry Insight

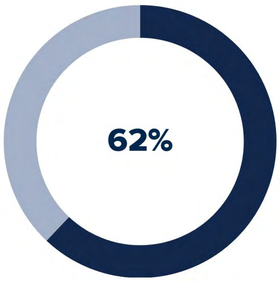
Having clear strategic priorities enables banks to guide their future plans, anticipate and respond to challenges and meet the needs of their customers and stakeholders. As banks experience increased competition and market pressure, many are exploring how AI and automation can help increase efficiencies to remain competitive, reduce operational costs and enhance customer experience. The continued theme of increasing efficiencies also plays into several other strategic priorities identified, including cybersecurity and customer support.

Due to past economic strain and interest rates, banks are focused on capturing and growing deposit accounts. While U.S. bank deposits declined throughout 2022 and most of 2023, they did start recovering in late 2023.[5] Building strong relationships with customers is paramount as banks focus on deposit growth. In addition to the 10% that chose mergers and acquisitions as a top issue poised to affect the industry, 30% of bankers also view mergers and acquisitions as a strategic priority for their institution.

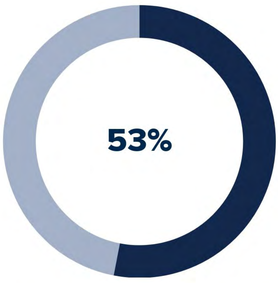
Embracing a Modern Core

While the rise of open banking enables faster implementation of third-party technologies, 89% of institutions prefer to get as much technology from one provider as possible, making selecting the right core provider even more important.

When asked how banks were planning to modernize their core banking solutions in the next 12 months, most bankers plan to invest in core or ancillary products that support ongoing innovation.

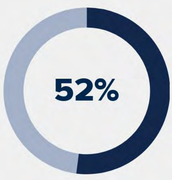


Investing in Core or Ancillary Products to Support Ongoing Innovation

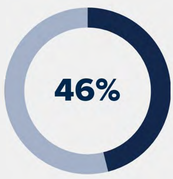


Evaluating Technology in Terms of Its Ability to Support Open Banking

Bankers also expressed interest in 24/7 real-time processing and migrating to a public cloud-based core. Only 2% of bankers surveyed expressed no plans to modernize in the next 12 months.



Implementing 24/7 Real-Time Processing



Migrating to a Public Cloud-Based Core System

Industry Insight

At its foundation, core modernization involves moving away from legacy applications towards web-based views and more user-friendly applications. The technology on which most legacy systems are built is reaching a point where it's unable to support the flexibility and adaptability banks require to stay competitive. As such, 98% of bankers expressed plans to modernize their cores in some way, with more than 60% pointing to investments in innovative core or ancillary products.

This modern approach allows institutions to reap a variety of benefits, including current technology, faster development and increased agility. Relatedly, Celent found that achieving speed and agility surfaced as a top driver of banks' technology investments as institutions rethink how technology solves business problems.[6] Respondents from institutions with asset sizes of $5B - $10B were most likely to select using or expanding use of integrated solutions supported by open APIs, highlighting the benefits open banking and APIs unlock relating to incorporating new technologies.

"In a rapidly changing world, the ability to adapt is not just an advantage; it's a necessity. Organizations that embrace change and foster a culture of flexibility are better positioned to navigate challenges and seize new opportunities."

Source: Survey Participant

Artificial Intelligence

AI is increasingly becoming a valuable tool for community banks, helping streamline operations and improve customer experience. Community banks typically have smaller budgets and fewer resources compared to larger national institutions, making AI a powerful ally in achieving efficiency. By automating repetitive tasks such as data entry, AI frees up staff to focus on higher-value, customer-focused activities.

Bankers widely understand AI and remain optimistic about its transformative potential in the industry. Those at institutions with an asset size between $1B - $5B were most likely to strongly agree about feeling optimistic about AI's potential.

89%

I understand what artificial intelligence is and how it can be used in banking.

88%

I am optimistic about the potential of AI in banking.

When asked how they envision applying AI in operations, bankers are interested in applications across business units.

91%

I would be interested in using AI for fraud and AML detection and prevention.

90%

I would be interested in using AI for customer service.

89%

I would be interested in using AI for sales/relationship management.

87%

I would be interested in using AI for back-office tasks.

Nevertheless, bankers have adopted a measured approach, as about eight in 10 are very or somewhat concerned about AI's potential in banking.

83%

I am concerned about the potential of AI in banking.

- This is a slight increase from last year when 73% reported concern.

Industry Insight

Institutions have deployed AI-driven chatbots and other customer communications for years, leading to increased levels of automation. Like last year's results, many respondents continue expressing measured optimism around AI, awaiting more use cases beyond these applications.

Due to AI's growing prominence in the industry, many regulatory bodies have been investigating various risks surrounding AI. Some have issued AI guidelines, frameworks and/or requirements around how banks should use and govern AI technology to help ensure responsible practices.[7] Banks should evaluate and implement AI governance recommendations to mitigate risk and establish clear guidelines for acceptable use.

Expert Perspective

It's been nearly two years since ChatGPT emerged, and a recent industry report shows about half of banks are actively investing in exploring generative AI use cases and working to understand the capabilities and risks of this technology.[8] GenAI can leverage vast amounts of unstructured data and can produce content and answers quickly. In contrast, discriminative AI is often used in more straightforward classification tasks such as spam detection, image recognition or risk prediction and mostly requires structured data (typically quantitative) to operate.

As institutions develop their GenAI strategies, it's critical to be mindful of security. Securing your data is critical to ensure that your AI engine is not training on any confidential information and your sensitive files are protected. As referenced earlier, banks should implement AI governance and risk management frameworks to ensure compliance and data security. With thoughtful implementation, AI has the potential to benefit banks, from delivering services at scale to identifying network vulnerabilities.

Top Technology Investments

This year's survey responses show financial institutions' continued commitment to engage digital-first consumers and provide a convenient, quick and simple banking experience.

Thanks to choices provided by open banking, bankers can partner with their core provider for the latest technologies or work with third parties for integrations. Take a deeper dive into bankers' thoughts on technology investments for 2025.

Top Technology Priorities

Read more

Digital Engagement

Read more

Open Banking

Read more

Automation in Lending

Read more

Payment Priorities and Trends

Read more

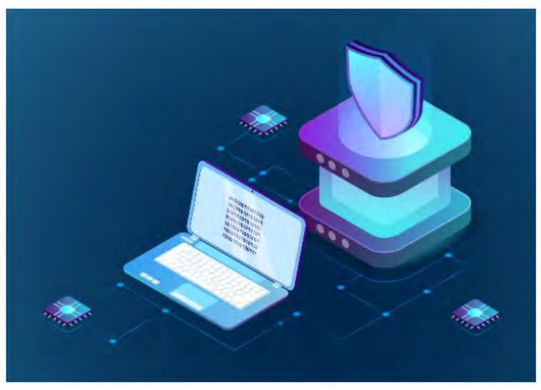
Cybersecurity

While today's digital-first world supports constant connectivity and convenience, it also opens up financial institutions to vulnerabilities and evolving cyber risk. Instead of gravitating towards a breakout issue, bankers' forward-looking cybersecurity concerns were divided.

This year's survey also delved into bankers' perceptions of cybersecurity readiness and tools for cybersecurity compliance, with results demonstrating bankers' commitment to security and areas of concern.

Cybersecurity Concerns on the Horizon

Read more



Banks Assess Cybersecurity Readiness

Read more

Focus on Cybersecurity Compliance

Read more

Forging Ahead in the Fight Against Fraud

As consumers increasingly rely on technology for financial activities, bad actors take advantage of expanding opportunities to execute fraud. To cope, banks and consumers must exercise continued awareness and education. Credit and debit card fraud losses peaked at $34.36 billion in 2022 as financial institutions face an environment rife with financial crime.[14]

CSI's 2025 survey explored the prevalent types of fraud encountered by financial institutions and assessed the effectiveness of current prevention measures.

Common Types of Fraud

Among the most reported fraud types, card fraud, check fraud, fraudulent account opening and wire transfer fraud emerged as primary concerns.

Over four in ten banks identified **card fraud (44%)** and **check fraud (44%)** as the foremost challenges.

Fraudulent account opening (40%) and **wire transfer fraud (39%)** closely followed.

Additional types include **account takeover (33%), P2P fraud (33%), phishing (31%)** and **insider threat (26%).**

Fraud Prevention Effectiveness

While banks expressed concern about fraud, they are also generally confident in the effectiveness of their prevention measures.

Card and Check Fraud

Card and check fraud both ranked as the most common types of fraud institutions face, with 44% of bankers choosing these options. Approximately three-quarters of banks surveyed feel their prevention measures for card and check fraud are highly or very effective.

Card Fraud Prevention Measures

33% Highly Effective

41% Very Effective

18% Moderately Effective

4% Slightly Effective

Check Fraud Prevention Measures

41% Highly Effective

34% Very Effective

17% Moderately Effective

4% Slightly Effective

As one of the oldest and most persistent forms of financial crime, it seems check fraud may never go out of style. In September 2024, a trend on social media exploded in which people claimed to have unlocked a "money glitch" in a major U.S. bank's ATM, only to later discover they had engaged in traditional check fraud. This resulted in significant consequences, including account holds and legal repercussions. Check fraud can also take the form of forgery, counterfeit or altered checks or check kiting.

Fraudulent Account Opening

Fraudulent account opening was another common type of fraud encountered by institutions, with 40% of respondents selecting this option. Fortunately, 75% of respondents agree their fraudulent account takeover prevention methods are effective.

Fraudulent Account Opening Prevention Measures

32% Highly Effective

43% Very Effective

18% Moderately Effective

5% Slightly Effective

Wire Transfer Fraud

Wire transfer fraud was also among the most prevalent types, with 39% of respondents selecting this option. Encouragingly, 78% of respondents believe that their wire transfer fraud prevention measures are highly or very effective.

Wire Transfer Fraud Prevention Measures

36% Highly Effective

42% Very Effective

15% Moderately Effective

3% Slightly Effective

Wire transfers remain popular with fraudsters due to their speed and finality. Despite these vulnerabilities, more than seven in 10 respondents feel their wire transfer fraud prevention measures are effective. Defending against wire fraud demands ongoing vigilance and a commitment to refining strategies. It is difficult to recover lost funds in wire fraud, so institutions should continue education to employees and consumers.

Industry Insight

Check fraud continues to plague institutions, with FinCEN reporting $688 million in reported suspicious activity related to mail theft-related check fraud.[15] Further, FTC data showed consumers reported fraud losses totaling more than $10 billion in 2023.[16]

While only 31% identified phishing as a common type of fraud, it remains a popular tool to perpetuate fraud schemes. It's critical that institutions continue educating consumers on common phishing schemes. Account takeover is another issue, growing more concerning given the rise in synthetic identities. To combat this, many institutions are embracing modern identity verification methods. When it comes to verification, there's can be a tradeoff between friction and security, but using methods like ID uploads and biometric authentication accelerates onboarding and reassures customers.

Expert Perspective

AI-powered fraud detection and prevention tools empower institutions in the fight against financial crime. AI can ingest and analyze more data than a traditional fraud tool, leading to more efficient decisioning and fraud identification. As fraud trends change, models must also adapt, which they can easily do if powered by AI. By enabling real-time detection, AI fraud tools accelerate investigation and help institutions limit their financial losses.

Financial institutions should proactively educate their customers about misinformation and nefarious financial schemes. Scams and dubious "hacks" circulate quickly on social media, but institutions that provide consumers with information can mitigate while increasing the potential for new business as a trusted resource.

Top Regulatory Issues

Regulatory change emerged as a top issue on bankers' minds, with 14% selecting this as the issue most likely to affect the financial industry. 2025 is poised to be a hot regulatory year with numerous recent developments.

Nearly three-quarters of financial professionals expressed concern about the Community Reinvestment Act (CRA). Financial crimes compliance was also at the top of the list with 74% reporting concern, likely due to recent updates to the AML Act of 2020 and increasing interest in AI.

74% Community Reinvestment Act (CRA)

74% Financial Crimes Compliance

73% Cloud-Based Banking Technologies

71% Cybersecurity Compliance

70% Building a Financial Services Ecosystem

70% Monetizing Data

68% Cryptocurrencies

68% UDAAP

66% CFPB's Rule 1033

Community Reinvestment Act (CRA)

74%
Concerned or Very Concerned

The Community Reinvestment Act (CRA) was modernized in October 2023, and banks continue adjusting to the new regulatory environment it creates.[17] CRA updates include encouraging banks to expand banking services access in low- and moderate-income neighborhoods, adapting to technological advancements and tailoring CRA evaluations and data collection by bank demographics. Most requirements become applicable by 2026, so banks are focusing on this to ensure sufficient information for CRA reporting.

28% Very Concerned
46% Somewhat Concerned
22% Concerned nor Not Concerned
4% Not Very Concerned
0% Not at all Concerned

Financial Crimes Compliance
(AI, Analytics, Fraud Detection, BSA/AML Modernization)

74%
Concerned or Very Concerned

The AML Act of 2020 touches upon using AI as a tool to enhance compliance capabilities for financial institutions. Regulatory bodies, including FinCEN and other federal agencies, recognize AI's potential to strengthen AML/CFT efforts, particularly in monitoring transactions, assessing risk and detecting suspicious activities in real time.

In 2024, FinCEN announced a proposed rule to strengthen institutions' AML/CFT programs by requiring that such programs be "effective, risk-based, and reasonably designed, enabling financial institutions to focus their resources and attention in a manner consistent with their risk profiles."[18]

32% Very Concerned
42% Somewhat Concerned
20% Concerned nor Not Concerned
5% Not Very Concerned
1% Not at all Concerned

Cloud-Based Banking Technologies

73%
Concerned or Very Concerned

Cloud-based banking technologies deliver a variety of benefits, including scalability and efficiency but regulatory implications exist as well. As banks partner with different providers for cloud-based technologies, prioritizing risk management, due diligence and compliance with regulatory requirements is key.

An FFIEC joint statement encourages financial institutions to engage in effective risk management around cloud computing and to understand "shared responsibilities between cloud service providers and their financial institution clients."[19]

29% Very Concerned
44% Somewhat Concerned
24% Concerned nor Not Concerned
4% Not Very Concerned
0% Not at all Concerned

Cybersecurity Compliance

71%
Concerned or Very Concerned

Bankers face ongoing cybersecurity challenges, especially as fraud and cyber threats remain top of mind. Focusing on cybersecurity compliance prepares banks to respond effectively to new and evolving threats—all while maintaining resiliency and compliance in an evolving regulatory environment. Preventative measures like ransomware self-assessment tools, cyber insurance and multi-factor authentication help institutions strengthen their security.

31% Very Concerned
40% Somewhat Concerned
23% Concerned nor Not Concerned
4% Not Very Concerned
2% Not at all Concerned

Building a Financial Services Ecosystem
(Fintech/Big Tech Partnerships, Third-Party Risk Management, Open Banking)

70%
Concerned or Very Concerned

Creating a financial services ecosystem includes developments in open banking as data is shared between multiple entities. As banks develop their open banking strategies, risk management and governance should be their guiding pillars. Regulatory agencies expect institutions to have strong risk management and governance programs in place—including robust vendor due diligence processes—to build the structural framework of their cybersecurity and compliance programs. As open banking becomes more prevalent, banks must ensure that any third-party partners adhere to regulations and use customer data only for intended purposes.

25% Very Concerned
45% Somewhat Concerned
24% Concerned nor Not Concerned
5% Not Very Concerned
1% Not at all Concerned

Monetizing Data
(Product and Service Optimization, Revenue Maximization)

70%
Concerned or Very Concerned

Banks can monetize data in various ways, including leveraging targeted advertising, engaging in personalized marketing or providing anonymized datasets to third-party organizations or researchers. However, institutions should approach this carefully by balancing data utilization with privacy considerations. A range of regulations from different agencies govern data use, whether for developing new products and services or for potential data resale. Adhering closely to these privacy standards and honoring customer preferences is essential for maintaining compliance and building trust with the customer base.

27% Very Concerned
43% Somewhat Concerned
24% Concerned nor Not Concerned
5% Not Very Concerned
1% Not at all Concerned

Cryptocurrencies

68%
Concerned or Very Concerned

Due to headlines about crypto-enabled financial crime, the collapse of crypto firm FTX and subsequent revelations of fraudulent practices, this field remains a polarizing topic. Last year's results indicated that 84% of bankers were concerned or very concerned about cryptocurrencies, so concern has dropped looking ahead to 2025. Banks should continue to keep an eye on crypto-related guidance from the FDIC, OCC and other entities.

30% Very Concerned
38% Somewhat Concerned
24% Concerned nor Not Concerned
6% Not Very Concerned
2% Not at all Concerned

UDAAP
(Fair Lending, Overdraft, Junk Fees)

68%
Concerned or Very Concerned

The FDIC and CFPB continue to focus on Unfair, Deceptive, or Abusive Acts or Practices (UDAAP), particularly addressing Non-Sufficient Funds (NSF) fees and the CFPB's concerns about "junk fees," such as return deposit item fees. Over the past few years, CFPB's reforms have resulted in $3.5 billion in annual savings on overdraft fees and an additional $2 billion in savings on non-sufficient funds fees.[20]

25% Very Concerned
43% Somewhat Concerned
27% Concerned nor Not Concerned
4% Not Very Concerned
1% Not at all Concerned

CFPB's Rule 1033
(Open Banking)

66%
Concerned or Very Concerned

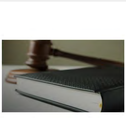
In October 2024, the CFPB issued a final rule to implement section 1033 of the Consumer Financial Protection Act of 2010 to strengthen consumers' financial data rights.[21] Rule 1033 requires financial institutions and other data providers to help consumers access and share their data securely using application programming interfaces (APIs). The rule covers financial data housed at banks, credit unions and other financial institutions, as well as payments apps and digital wallets. As APIs become more important in our financial landscape, banks will likely be navigating new cybersecurity and privacy rules in the coming years.

29% Very Concerned
37% Somewhat Concerned
25% Concerned nor Not Concerned
8% Not Very Concerned
1% Not at all Concerned

Industry Insight

AI continues as a recurring theme in this year's report, driven in part by the AML Act of 2020. AI improves efficiency by analyzing vast data sets, reducing false positives and streamlines compliance reporting, making it easier for financial institutions to meet BSA/AML requirements. However, institutions should keep in mind agencies will emphasize the need for transparency, auditability and data quality in AI models used for BSA/AML compliance.

While Rule 1033 only impacts banks with assets in excess of $850 million at this time, all banks should take note of this regulatory development. As consumers exercise more control over their data, they're able to more easily partner with banks that provide personalized service and their desired products. Institutions that embrace open banking and develop strategies that meet regulations can more easily offer new products or services to meet customer needs without building them internally or relying on a single provider.



The Future of Community Banking

The future of community banking is poised to blend traditional, relationship-based services with innovative digital solutions and experiences to meet evolving customer expectations. Technology continues to accelerate, and AI stands out as a transformative trend that enables banks to streamline operations and gain efficiencies.

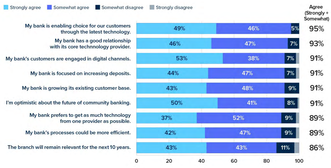
As digital threats become more frequent and sophisticated, banks must invest in robust training and security controls to protect sensitive data and maintain customer trust. Personalization will play an increasingly important role as consumers expect tailored, data-driven solutions similar to other retail experiences.

Moving forward, bankers' outlook remains optimistic and reflects a commitment to customer service. Despite the reliance on technology and digital tools shaping how consumers interact with financial institutions, community banks recognize the human element as their key differentiator. By balancing innovation and their core mission of delivering exceptional customer experiences, community banks are well positioned to deepen their relationships and continue driving economic growth.

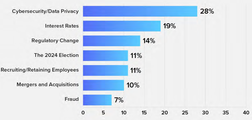
Appendix

CSI's annual Banking Priorities survey asks bankers about the most pressing issues, trends and strategies in the financial industry this year. Check out the detailed survey results in the charts below.

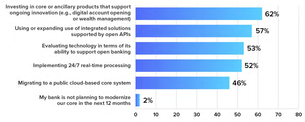
1. To what extent do you agree or disagree with the following statements?



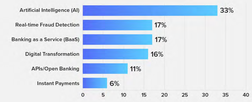
2. Which issue will most affect the financial industry in 2025? Please select the top issue.



3. How, if at all, is your bank planning to modernize your core banking solutions in the next 12 months?

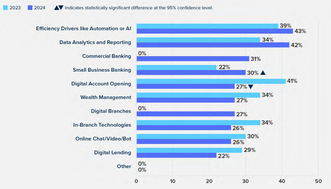


4. Which technology trend will most affect the financial industry in 2025?

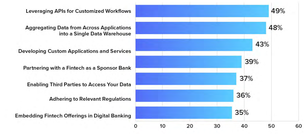


5. What are your institution's top 3 strategic priorities for 2025? Please select three options.

6. Which 3 technologies will your institution prioritize in 2025? Please select three options.

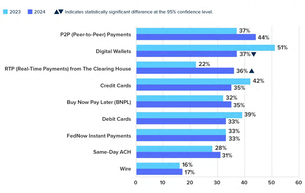


7. What are your institution's primary goals for implementing Open Banking APIs? Please select all that apply.

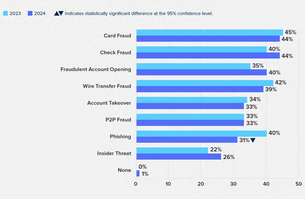


8. In what areas would automation in lending benefit your bank's operations?

9. Which 3 payment technologies will your institution focus on in 2025? Please select three.

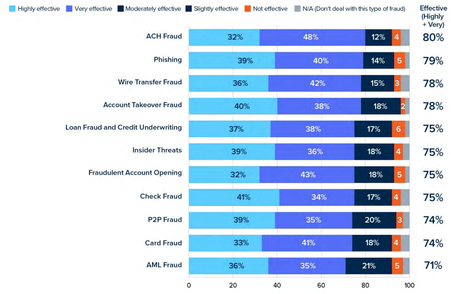


10. What are the most common types of fraud your institution encounters? Please select all that apply.

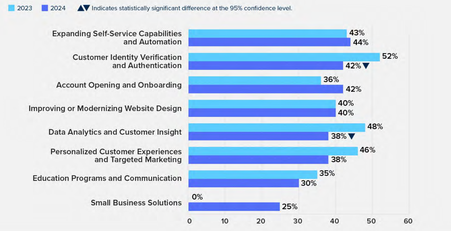


(continued on next page)

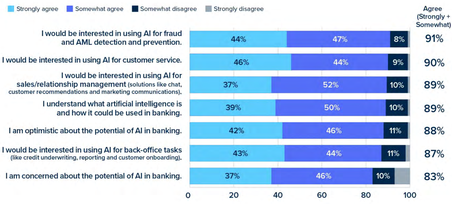
11. How effective are your current fraud prevention measures in mitigating these risks? Please rate the effectiveness of your prevention measures for each. If you are not currently using a measure, please select Not Applicable.



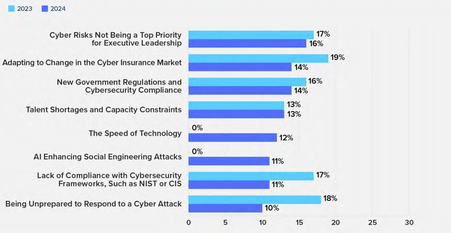
12. What are your top 3 priorities for enhancing digital customer engagement in 2025? Please select three.



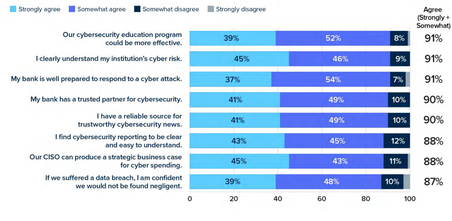
13. To what extent do you agree with the following statements? (Please rate on a scale of 1-5, with 1 being strongly disagree, and 5 being strongly agree).



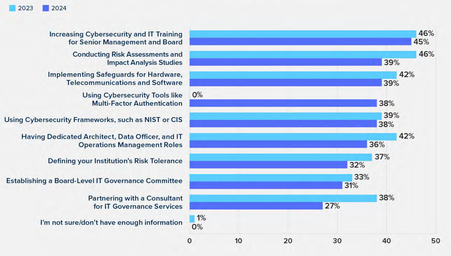
14. What is your greatest forward-looking cybersecurity concern? Please select one.



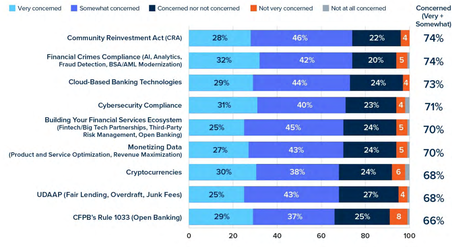
15. For each statement, mark whether you agree or disagree. (Please rate on a scale of 1-5, with 1 strongly disagree and 5 being strongly agree).



16. What tools and resources does your institution use to ensure cybersecurity compliance? Please select all that apply.



17. Please rate your level of concern for the following regulatory issues (1-5, with 1 being least concerned and 5 being the most concerned)?



Resources

About CSI

As a forward-thinking software provider, CSI helps community and regional banks, as well as organizations worldwide, solve their customers' needs through open and agile technologies. In addition to its nearly 60-year reputation for personalized service, CSI is shaping the future of banking by swiftly deploying advanced solutions that help its customers rival their competition.

---

[1] IBM, Cost of a Data Breach Report 2024

[2] Juniper Research, Open Banking Opportunities, Competitor Leaderboard & Market Forecasts 2023-2027

[3] The Financial Brand, How Banks Can Unlock the Complete Value of Automation

[4] Forbes, 22 Top AI Statistics and Trends in 2024

[5] McKinsey, US Banks' Commercial Deposits are Back on a Path to Growth

[6] Celent, Build for Today, But Design for Tomorrow: Modern Architecture for Corporate Banking

[7] Celent, AI and Data Governance: A New Era for Banks

[8] Celent, GenAI: Beyond the Proof of Concept – Banking Edition

[9] Datos Insights, Consumers' Lending Preferences: And Financial Institutions' Plans to Satisfy Them

[10] CBS News, Americans Continue to Rack Up Credit Card Debt, Hitting a Record $1.14 Trillion

[11] PYMNTS, Gen Z Relies More on BNPL for Small, Everyday Purchases

[12] FedNow, One Year After Launch: Broad Range of U.S. Financial Institutions See Benefits of Joining the FedNow Service

[13] Deloitte, Generative AI is Expected to Magnify the Risk of Deepfakes and Other Fraud in Banking

[14] WalletHub, Credit Card Fraud Statistics

[15] FinCEN, FinCEN Issues In-Depth Analysis of Check Fraud Related to Mail Theft

[16] Federal Trade Commission, As Nationwide Fraud Losses Top $10 Billion in 2023, FTC Steps Up Efforts to Protect the Public

[17] FDIC, Agencies Issue Final Rule to Strengthen and Modernize Community Reinvestment Act Regulations

[18] FinCEN, FinCEN Issues Proposed Rule to Strengthen and Modernize Financial Institutions' AML/CFT Programs

[19] FDIC, FFIEC Joint Statement on Risk Management for Cloud Computing Services

[20] CFPB, CFPB Proposes Rule to Close Bank Overdraft Loophole that Costs Americans Billions Each Year in Junk Fees

[21] CFPB, Required Rulemaking on Personal Financial Data Rights

Bankers' Top Technology Priorities

Community financial professionals had diverse responses when asked about their top three technology investments for 2025. The responses shifted somewhat compared to previous years, highlighting the changing nature of technology.

Efficiency drivers like automation and AI topped bankers' list of technology priorities, followed closely by data analytics and reporting. Institutions with assets between $500M - $1B were more likely to select the top two options.

43%
Efficiency Drivers like Automation or AI

42%
Data Analytics and Reporting

Commercial banking, small business banking, digital account opening, wealth management and digital branches clustered together with moderate attention.

31%
Commercial Banking

30%
Small Business Banking

27%
Digital Account Opening

27%
Wealth Management

27%
Digital Branches

The last three options rounded out the group.

26%
In-Branch Technologies

26%
Online Chat/Video/Bot

22%
Digital Lending

Industry Insight

Banks continue competing for consumers and talent, leading to 43% prioritizing efficiency drivers that enable them to do more with less. Most banks are seeking efficiencies in back-office processes, with some beginning to utilize AI and automation to remove manual steps and add new functionality.

Data analytics and reporting provides banks with insight to understand customer behavior and identify areas to better serve them, including customizing offerings and promoting them via the digital experience. Analyzing data to create a personalized experience for customers to meet their needs also helps institutions solidify relationships and decrease attrition.

Expert Perspective

Compared to last year's 22%, interest in small business banking increased and represents potential for driving fee revenue, along with commercial banking. By targeting existing customers with small business banking solutions, institutions can lower acquisition costs and deliver seamless personal and business banking experiences.

Meanwhile, it's possible that banks have already invested in digital account opening, wealth management solutions, in-branch technologies, online chat/video/bot and digital lending solutions or that the interest environment has shifted these to lower priorities for some institutions.

Return to main section

How Banks are Delivering on Digital Engagement

Customers expect a seamless digital experience across all channels, and banks must engage new and existing customers to maintain a competitive edge.

Bankers selected a few priorities to elevate digital engagement in 2025:

44%

Expanding Self-Service Capabilities and Automation

44% of bankers are prioritizing expanding self-service capabilities and automation to increase digital engagement among customers. This includes deploying tools that enable customers to complete their banking activities with little friction.

42%

Customer Identity Verification and Authentication

While this is a drop from last year's 52%, that could indicate banks have made strides to implement this technology over the last 12 months. Customer identity verification helps increase security while solving the need for self-service capabilities among consumers.

42%

Account Opening and Onboarding

About four in 10 bankers also recognize the need for streamlining the account opening process, enabling new or existing customers to complete the process digitally. Optimizing account opening leads to increased engagement and adoption of further digital experiences.

While the top three priorities stand out, the survey also reveals other areas of focus trailing closely behind:

40%

Improving or Modernizing Website Design

38%

Data Analytics and Customer Insight

38%

Personalized Customer Experiences and Targeted Marketing

30%

Educational Programs and Communication

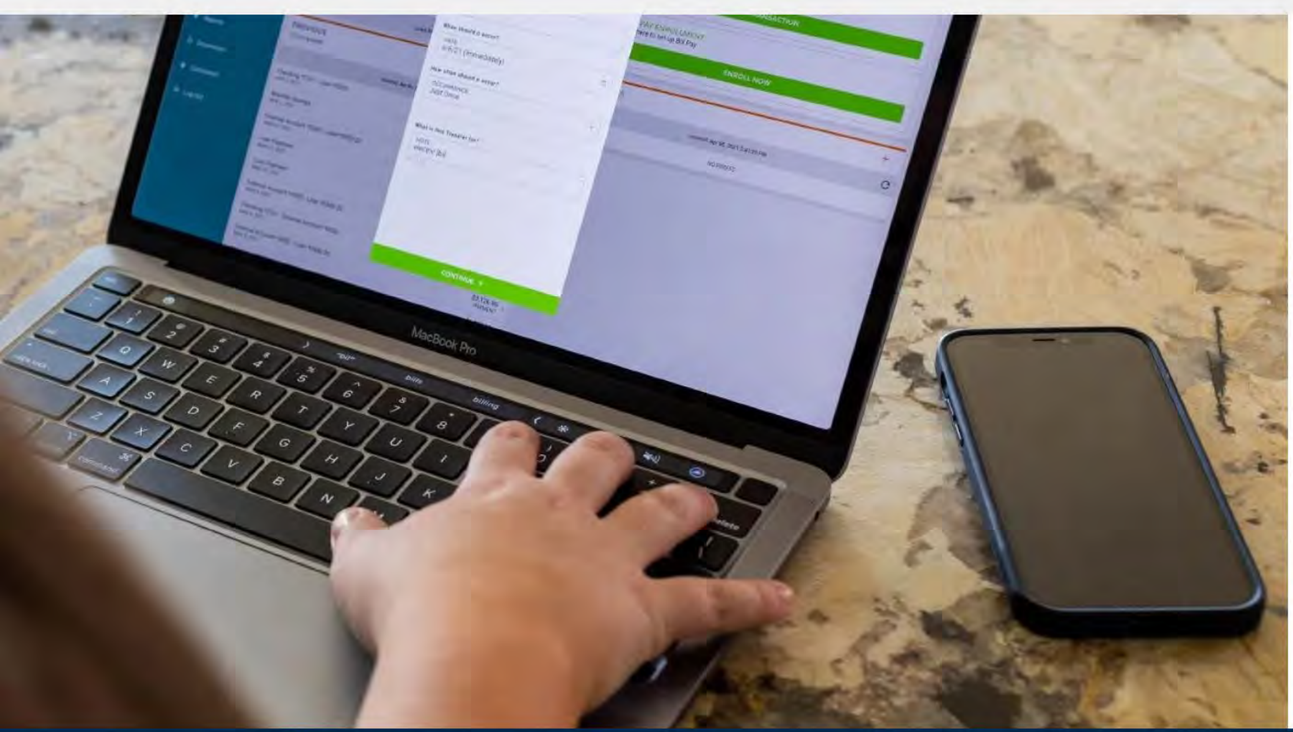
25%

Small Business Solutions

Industry Insight

Since digital channels encompass much of a user's experience, many of these engagement priorities are connected as part of a bank's greater digital strategy. Bankers' responses indicate their focus on creating seamless digital experiences for customers, from enabling self-service capabilities to intuitive onboarding and account opening. Automation continues to emerge as a theme among this year's responses, and bankers are continuing to focus on automation in digital engagement to streamline processes.

Nearly 40% of bankers report interest in using data analytics and customer insight, and these tools can help institutions develop and deliver personalized marketing initiatives to break through the noise and reach new and existing customers. Data analytics can also be used to provide easily digestible insight to consumers about their own financial health, allowing banks the opportunity to highlight education and communication around financial best practices. A quarter of bankers are also exploring small business solutions to increase deposit growth and foster additional engagement.



Expert Perspective

In today's digital-first world, consumers expect a streamlined, frictionless experience, and digital account opening and onboarding is no different. Optimizing the digital account opening experience enables customers to choose how, when and where they bank, leading to a stronger relationship with their financial institution.

Providing personalization throughout the digital experience is the core of digital engagement. To improve digital engagement, banks should strive to provide unique solutions to best serve customers and increase the adoption of those services. The more personalization banks build into their products and experiences, the more they will drive engagement, adoption and loyalty. Personalization builds trust, leading to less attrition and increasing the adoption of new products.

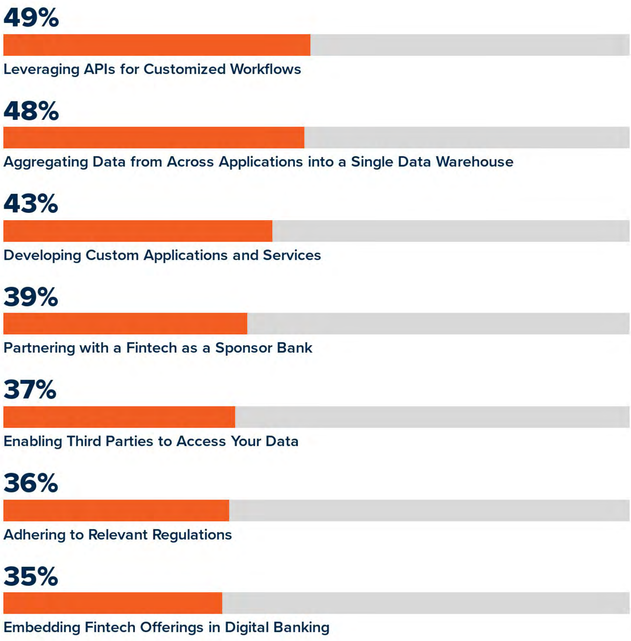
Return to main section

Open Banking

95% of bankers strongly or somewhat agree that they are enabling choice for customers through the latest technology. For many, that means embracing open banking to streamline processes and offer solutions outside of those from their primary technology provider.

Open banking facilitates enhanced collaboration between banks and fintech service providers by connecting them via Application Programming Interface (API) software. This practice has surged in recent years, demonstrated by bankers' continued interest and adoption.

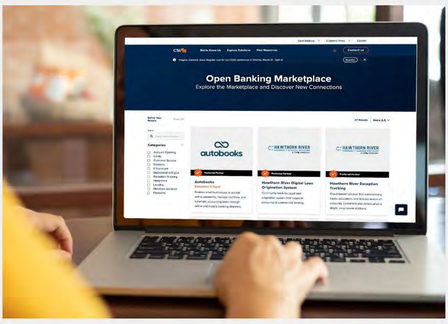
When asked to select their open banking goals, bankers responded that they are:



Industry Insight

The case for open banking lies in the potential for adaptability, choice and increased efficiencies. Open banking APIs facilitate real-time data movement, providing institutions with increased functionality that supports efficiencies and an improved customer experience. Banks can now choose applications that will open different revenue streams and align with services their customers desire that partnering fintechs can provide.

With CFPB's Rule 1033, consumers have more control over their data and how they interact with financial institutions. Although institutions with assets below $850 million are not included in the final rule, those that adapt and facilitate data sharing for consumers using APIs stand to become more competitive as consumers' expectations evolve.



Expert Perspective

As the results indicate, most banks recognize the transformative potential of open banking. Banks interested in beginning or continuing their open banking journey should first assess where they are in terms of their current technology and resources. Then, identify efficiencies or product gaps, research the best solutions and deploy an integration. Once one integration is successfully deployed, banks can look at other areas and build their integration set. Starting small and building allows banks to more easily manage vendor due diligence, compliance and business goals.

As banks evaluate potential technology partners, they should ask:

- **Who:** Who is moving the data? Which applications are required for the process?
- **Where:** Where is the data moving from and where is it going?
- **What:** What data is moving?

Having a full understanding of these areas will set banks up for success on their open banking journey. Institutions should also conduct a thorough due diligence process, exercising caution when working with fintechs that can't provide proof of industry experience or standard security documents.

Return to main section

Automation in Lending

Lending is a considerable revenue source for many institutions, so ensuring a speedy and simple lending process to satisfy customers and support employees is critical.

We asked bankers to identify the areas in which their institutions would benefit from automation in lending operations. Responses reveal that all bankers surveyed believe automation would be a boon to lending operations in some way.

46%

Digital Engagement with Customers

As consumers continue using digital channels, it's no surprise 46% of respondents identified digital engagement as the primary benefit of lending automation. Embracing automation in lending enables banks to facilitate greater digital engagement since many consumers prefer a digital-first approach. With an automated, modern loan origination platform, banks are meeting customers where they are and enabling online loan applications, document uploads and electronic signatures.

42%

Regulatory Compliance

42% of banks identified regulatory compliance as an area in the lending process that would benefit from automation. Automating reporting and tracking supports consistent, standardized processes for lending activities and flags any anomalies or potential compliance issues in real time. Further, automation enables standardized data capture for more accurate compliance, as well as streamlining preparedness for upcoming exams.

40%

Credit Scoring and Decisioning

Four in 10 bankers responded that automating credit scoring and decisioning would benefit their lending operations. This doesn't necessarily mean completely automated decisioning, but decision recommendation that falls within determined guidelines. When exploring automation in this area, it's important that banks consider fair and consistent application, including human oversight and intervention. Annual review of scoring models and any applicable adjustments based off current economic conditions should also be conducted.

38%

Data Entry and Analysis

Automating data entry and analysis helps streamline this common process, and 38% of bankers selected this option. Multiple platforms lead to complicated integrations and numerous places to input data, often leading to duplicate data entry among staff becoming an unfortunate reality. With already strained resources, this is a significant drag on operational efficiencies and represents increased risk since opportunities for mismatched data rise with each manual entry.

In addition to the top four benefits, the survey also reveals other areas trailing closely behind:

37%

Risk Assessment

33%

Document Imaging and Verification

31%

Customer Onboarding

23%

Tickler Management

18%

Underwriting

Industry Insight

Institutions appear to agree that optimizing digital experiences and engagement throughout the lending process is a priority. According to Datos Insights, 88% of U.S. lenders planned to increase or maintain their "digital borrowing experience" budget in 2023 compared to previous years.[9] Banks who fail to meet customers or prospects in the digital space miss out on business opportunities and revenue. A single platform for managing and monitoring lending is critical for banks in today's digital-first environment.

Expert Perspective

A modern, automated loan origination system affords banks scalability and flexibility with lending, supporting long-term growth. Banks considering modernizing their approach should start small and then continually improve. Accounting for an institution's current size, growth trajectory, available resources and future goals helps inform the path forward with implementing automation and advanced lending technology.

Return to main section

Payment Priorities and Trends

Digital-first trends continue as bankers shed light into the modern payments landscape in their responses.

To meet consumers' preference for convenient, quick payments, bankers are embracing modern payments technologies.

Ranking Payments Technologies by Priority and Interest

Bankers were asked to select their top three payment priorities for 2025.

Peer-to-Peer (P2P) Payments

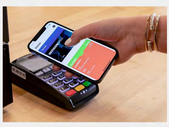
44%

While slightly higher than the previous year's ranking of 37%, P2P payments are bankers' top focus for 2025, highlighting the importance of convenience for person-to-person payments. By offering P2P payments and meeting customers' needs, banks are better positioned to become the top-of-mind financial partner for customers.

Digital Wallets

37%

Digital wallets received less attention compared to last year's 51%, but that could be a result of increased execution and adoption of this technology. For banks that haven't yet prioritized digital wallets, this could indicate they need to evaluate this space. Investment in this technology could also lead to additional interchange revenue from credit and debit cards that are used in digital wallets.



Real-Time Payments from The Clearing House

36%

36% of bankers selected real-time payments (RTP) from The Clearing House, a significant increase from last year (22%). Bankers continue to take note of the advantages of payments that process immediately.

Credit Cards

35%

At 35%, credit cards remain a priority for bankers. This isn't a surprise given consumers' increased use of credit-related products to manage spending in today's economic landscape. By August of 2024, U.S. credit card debt reached $1.14 trillion, growing by $27 billion compared to the second quarter of the year.[10] This is likely due to economic uncertainty, inflation and interest rates and suggests Americans are using credit cards to carry more debt for longer periods of time.

Buy Now Pay Later (BNPL)

35%

BNPL has emerged as a priority for the past two years, with a slight increase compared to last year's results at 32%. According to PYMNTS, millennials and Gen Z often spend more using BNPL compared to credit cards.[11] This result represents an opportunity for banks to explore embedding an installment plan as a post-purchase liquidity strategy when a customer uses a debit or credit card for a larger transaction.

Debit Cards

33%

Debit cards remain relevant among bankers as a core payment technology and interchange revenue driver for surveyed institutions.

FedNow Instant Payments

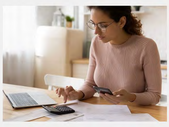
33%

Instant payments from the FedNow Service®, which launched in 2023, captured bankers' interest and mirrored last year's results at 33%. Since its launch, more than 900 financial institutions have connections to the FedNow Service. According to the Fed, community banks and credit unions comprise nearly 80% of total participating financial institutions.[12]

Same-Day ACH

31%

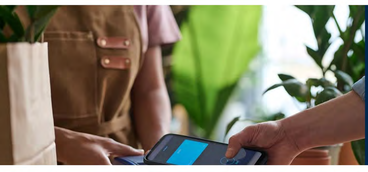
Same-Day ACH captured moderate attention, reflecting the industry's acknowledgment of the continued importance of expediting ACH transactions.



Wire Transfers

17%

As adoption of instant payments increases, industry experts anticipate a coming shift in payment preferences, including decreased use of wire transfers and same-day ACH.



Industry Insight

Each of the payment options discussed above plays a part in an institution's goal of becoming and remaining a customer's primary choice for money movement. Having payments technology—like P2P, digital wallets or debit and credit cards—that consumers desire allows institutions to bridge the day-to-day transactions and become the first choice when additional financial needs arise, such as mortgages, personal loans or car loans. Institutions' prioritization of P2P payments and digital wallets align with consumers' preferences for seamless, quick payments.

Expert Perspective

As banks continue to leverage credit and debit cards as a component of their payments strategy, enhanced security and risk management should remain a priority. As a result of increased e-commerce activity, chargebacks have recently increased. It's estimated that chargebacks—the reversal of funds that occurs when a customer disputes a transaction—totaled $100 billion in 2023. Scammers use fraudulent transactions to request chargebacks, often leading to headaches for financial institutions and requiring increased security measures like tokenization.

This year's results also indicate bankers' interest in real-time or instant payments. The primary difference in real-time or instant payments is the operator of the payment system. The Clearing House was first to market in 2017 with its RTP®, a service operated by a group of large commercial banks. The U.S. Federal Reserve operates FedNow, an instant payments network designed to provide secure, fast payments for all financial institutions. As interest increases in modern payments, banks should seek out technology providers prioritizing payment technologies.

Return to main section

Cybersecurity Concerns on the Horizon

How do bankers feel about ever-evolving cybersecurity threats? When asked to choose their top cybersecurity concern, bankers revealed a cluster of issues rather than one primary standout.

Below we explore the cybersecurity concerns at the forefront of bankers' minds going into 2025:

Cyber Risks Not Being a Top Priority for Executive Leadership

Cybersecurity is a business issue, requiring the attention of a financial institution's leadership for effective prevention and risk mitigation. By prioritizing cyber risk, executive leaders can play a role in protecting their institution's assets, ensuring compliance with evolving regulations and maintaining the trust of customers.

Adapting to Changes in the Cyber Insurance Market

Cyber insurance helps financial institutions mitigate their risk against the escalating costs associated with cyber incidents. Despite the average cost of a data breach in the financial industry reaching $6.08 million, the cyber insurance market that was previously driven up by ransomware spikes has stabilized over the past year. Institutions should review their coverage to understand the specifics, and IT governance services can help evaluate needs and coverage.

New Government Relations and Cybersecurity Compliance

The regulatory environment is constantly evolving, leading many bankers to express concerns with increasingly stringent cybersecurity compliance requirements. As more laws emerge related to data privacy, banks must balance compliance and risk management while staying ahead of the latest threats.

Talent Shortages and Capacity Constraints

Talent shortages, especially in cybersecurity, have been a trend for years among financial institutions. It can be competitive and expensive for banks to attract and retain forward-thinking, experienced cybersecurity talent. Cybersecurity teams are often tasked with monitoring and remediating security events, leading to capacity constraints as threats grow. Many institutions turn to trusted managed cybersecurity providers to help bridge this gap.

The Speed of Technology

Given the fast pace at which technology evolves, banks often need a trusted advisor to help them keep up. It's becoming increasingly difficult for banks to navigate the technology landscape alone due to AI-driven developments and accelerated threats. Further, the speed of technology doesn't always align with an institution's budget cycle, leading to delays in obtaining the technology needed to address current threats.

AI Enhancing Social Engineering Attacks

Cybercriminals use AI to speed up their malicious efforts and increase effectiveness of attacks, including social engineering. Cybercriminals no longer have to write their own phishing emails or scripts when AI can create them within seconds. It's also easier for cybercriminals to launch personalized phishing attacks, as automation leads to increased speed and scalability. Institutions should stay informed of the latest trends to mount the most effective defenses.

Lack of Compliance with Cybersecurity Frameworks

Cybersecurity frameworks, such as the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF), provide institutions with ways to identify and implement solid controls in high-risk areas. Best practices like the Center for Internet Security (CIS) Critical Security Controls further strengthens institutions' compliance initiatives and cybersecurity spending.

Being Unprepared to Respond to a Cyberattack

While this response decreased from last year's at 18%, cyberattacks still plague financial institutions. It's imperative that institutions continue to focus on preparedness with robust Incident Response Plans (IRPs) that cover data and system backups, communication plans, business continuity plans and strategies for dealing with attackers. Advanced cybersecurity monitoring systems allow for swift identification and response to potential threats, reducing the likelihood of successful attacks.

Industry Insight

Despite valid concerns related to cybercriminals' adoption of AI for targeted, sophisticated attacks, this technology offers benefits for financial institutions as well. Automating certain tasks and cybersecurity responses leads to reduced errors and greater protection. While traditional cybersecurity methods may be slow to adapt to new or evolving threats, AI quickly adapts to identify new threats and elevates threat intelligence. Especially as these tools mature, AI stands to revolutionize cyber defense for financial institutions and other organizations.

Expert Perspective

Since community banks are already trusted partners, they are in a unique position to deepen relationships with customers by becoming a resource on cybersecurity best practices, common schemes and online safety. Social engineering stands to become more advanced with AI, especially as fraudsters expand their use of deepfakes, which are AI-generated audio or video clips. Considering deepfakes increased 700% in fintech in 2023, institutions should prioritize both cybersecurity training and detection methods.[13] By providing education on AI's perils and pitfalls, community banks can directly contribute to a stronger, safer community and customer base.

"Investing in cybersecurity is no longer optional; it's essential for safeguarding customer trust and ensuring long-term viability."

Source: Survey Participant

Return to main section

Banks Assess Cybersecurity Readiness

In addition to their cybersecurity concerns, bankers shared their perspectives on the landscape overall, as well as their own cybersecurity readiness.

- **91% agree** (with **39% strongly agreeing**) that their bank could improve cybersecurity education. However, just as many **(91%)** feel they understand their institution's cyber risk and believe they are well prepared to respond to a cyberattack **(91%)**.
- Although lower than other worries, only **87% agree** that their institution would not be found negligent if they suffered a data breach.

Bankers were given eight statements related to these issues and asked to provide their level of agreement. Their responses were as follows:

Our cybersecurity education program could be more effective.

91%
Agree (Strongly + Somewhat)

39% Strongly Agree
52% Somewhat Agree
8% Somewhat Disagree
0% Strongly Disagree

I clearly understand my institution's cyber risk.

91%
Agree (Strongly + Somewhat)

45% Strongly Agree
46% Somewhat Agree
9% Somewhat Disagree
0% Strongly Disagree

My bank is well prepared to respond to a cyberattack.

91%
Agree (Strongly + Somewhat)

37% Strongly Agree
54% Somewhat Agree
7% Somewhat Disagree
2% Strongly Disagree

My bank has a trusted partner for cybersecurity.

90%
Agree (Strongly + Somewhat)

41% Strongly Agree
49% Somewhat Agree
10% Somewhat Disagree
0% Strongly Disagree

I have a reliable source for trustworthy cybersecurity news.

90%
Agree (Strongly + Somewhat)

41% Strongly Agree
49% Somewhat Agree
10% Somewhat Disagree
0% Strongly Disagree

I find cybersecurity reporting to be clear and easy to understand.

88%
Agree (Strongly + Somewhat)

43% Strongly Agree
45% Somewhat Agree
12% Somewhat Disagree
0% Strongly Disagree

Our CISO can produce a strategic business case for cyber spending.

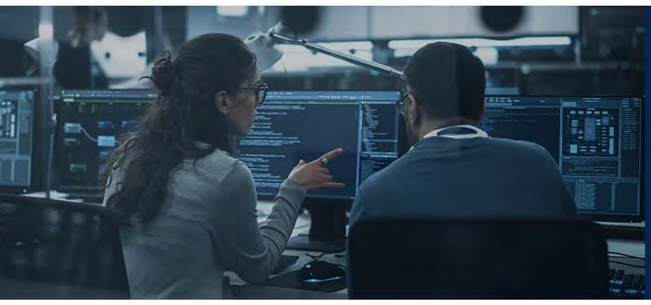
88%
Agree (Strongly + Somewhat)

45% Strongly Agree
43% Somewhat Agree
11% Somewhat Disagree
0% Strongly Disagree

If we suffered a data breach, I am confident we would not be found negligent.

87%
Agree (Strongly + Somewhat)

39% Strongly Agree
48% Somewhat Agree
10% Somewhat Disagree
1% Strongly Disagree



Industry Insight

CISOs can partner with trusted cybersecurity providers to develop use cases to ensure their cybersecurity controls and plans align with business goals. 90% of bankers strongly or somewhat agree that they have a trusted partner for cybersecurity indicates that many institutions are leaning on partners to help navigate cyber threats, regulatory requirements and more.

Expert Perspective

Given the risk cyber threats pose to institutions, it could only be beneficial for financial institutions to have internal discussions between their CISO and other C-suite executives to ensure alignment on these statements. A heightened focus on improving cybersecurity education for both employees and customers will better position institutions as cyber threats continue evolving. By rethinking cybersecurity education developing engaging and relevant training, institutions can cultivate a cyber-aware culture.

Return to main section

Cybersecurity Compliance

Regulators continue focusing on cybersecurity compliance, expecting institutions to maintain a secure IT infrastructure, actively mitigate risks and meet the complex regulatory requirements of the financial industry.

To determine how bankers approach cybersecurity compliance, we asked them to identify the tools and methods they prioritize in this area. The most selected tool used for cybersecurity compliance is increasing cybersecurity and IT training for senior management and boards of directors, followed by conducting risk assessments and impact analysis studies.

45%
Increasing Cybersecurity and IT Training for Senior Management and Board

39%
Conducting Risk Assessments and Impact Analysis Studies

39%
Implementing Safeguards for Hardware, Telecommunications and Software

38%
Using Cybersecurity Tools like Multi-factor Authentication

38%
Using Cybersecurity Frameworks, such as NIST CSF or CIS

36%
Having Dedicated Architect, Data Officer, and IT Operations Management Roles

32%
Defining Your Institution's Risk Tolerance

31%
Establishing a Board-Level IT Governance Committee

27%
Partnering with a Consultant for IT Governance Services

Industry Insight

At its core, cybersecurity compliance fulfills necessary regulatory requirements by implementing proven security controls to protect institutions. It's no secret that cybersecurity and IT training is important, and bankers should deploy a variety of strategies in this area to maximize effectiveness, such as gamification, interactive videos or scenario-based training.

Risk assessments and impact analysis studies fell slightly in priority compared to last year's results where it garnered 46% of the vote. While this is associated with meeting regulatory expectations, banks should embrace these exercises with the mindset of identifying the greatest risks and vulnerabilities. A well-managed cybersecurity compliance program can lead to relatively quick and painless exams while mitigating cyber risk.

Expert Perspective

Compared to last year's results, bankers' responses are lower across the board, which could indicate other priorities rising above cybersecurity compliance. These responses also suggest that bankers are missing opportunities to strengthen cybersecurity compliance and risk management. Specifically, deploying tools like multi-factor authentication (MFA) improves cybersecurity and compliance for institutions, and less than 40% of respondents report taking advantage of this protection. MFA adds an extra step to the login process, but in doing so it minimizes account takeover risk. Banks should deploy MFA as a tool to safeguard accounts, especially as hackers use AI to launch sophisticated attacks that lead to credential theft.

Return to main section