2026 Banking Priorities

Executive Report

Community financial institution leaders reveal their priorities, challenges and blueprints for success in 2026.

Read the report

Contents

Introduction to the 2026 Report 3
Community Banking Snapshot 4
Key Highlights and Preview 5
Top Issues on Leaders' Minds 6
Technology Trends for 2026 7
Technology in Commercial Banking 8
Institutions' Strategic Priorities 9
Artificial Intelligence (AI) 10
Top Technology Investments 11
Cybersecurity 12
Fighting Fraud on All Fronts 13
Top Regulatory Concerns 14
Conclusion 15
Appendix 16
Resources 20

2026: Banking's Next Frontier

Community Bankers Embrace an Era of AI and Increased Efficiency

The U.S. financial industry is entering a pivotal year. The pace of technological change, rising consumer expectations and growing risks are reshaping how community banks and credit unions operate.

Community financial institutions face intensifying pressure from multiple directions. Digital-first fintechs continue pushing upward from the low end of the market while larger banks continue moving down-market. High regulatory and compliance demands persist, while Gen Z and Millennials show less loyalty and greater digital expectations.

Despite these pressures, many financial institution leaders remain optimistic. From artificial intelligence (AI)—expected to have the biggest impact this year—and automation to digital-first payments and cybersecurity, they're embracing tools to modernize operations, increase efficiencies, mitigate risks, transform data into personalized interactions and strengthen account holder relationships.

This report explores how community banks and credit unions plan to navigate this next frontier, highlighting the priorities, challenges and technology strategies shaping 2026. As community institutions modernize and adapt, many aim to ensure new solutions strengthen their ability to serve account holders and maintain the relationship-driven approach that defines them.

About CSI's 2026 Banking Priorities Survey

Understanding where the banking industry is headed starts with listening to the leaders who shape it every day. That's why CSI conducts an annual survey of community and regional financial institutions across the country: to capture their priorities, challenges and technology plans for the year ahead.

These insights provide a clear view of trends and peer strategies, helping community financial institutions see where they're on track and where they may need to adjust.

Use this report as a practical guide for navigating 2026 with confidence and delivering the experiences that delight, protect and support your account holders.

Independent firm CITE Research conducted this eleventh annual survey in October 2025. Responses were gathered from 252 community banking professionals at manager level and above, from institutions nationwide, strategically dispersed across these demographics:

Institution Asset Size

17% $100M - $250M

21% $250.1M - $500M

26% $500.1M - $1B

23% $1.1B - $5B

13% $5.1B - $10B

Financial Institution Type

85% Community Bank

15% Credit Union

Role of Respondent

28% C-Level Executive

9% Senior Vice President

7% Vice President

25% Director

31% Manager

This interactive report reveals their responses, along with industry insight and expert perspectives, to provide a holistic outlook. All percentages are rounded to the nearest whole percentage point with an estimated margin of error of slightly over 6%.

Community Banking Snapshot

Community banks and credit unions (defined here as locally operated financial institutions with under $10 billion in assets) remain a cornerstone of the American financial system. They provide personalized services, support local businesses and help build economic stability in their communities.

Community Banking Heading into 2026

Consumer profiles are changing, and financial institutions must ensure they are prepared to meet a wide range of needs and expectations. Younger generations want fast, seamless and personalized digital services and aren't afraid to switch institutions to find them. Meanwhile, competition is intensifying from all directions, and expectations around cybersecurity, AI governance and fraud prevention continue to rise. To thrive, community banks and credit unions must stay agile, protect their account holders and use technology in ways that enhance—not replace—their personal service.

Confidence in Community Banking

Despite the many challenges they face, most banking professionals (especially those from larger institutions) remain optimistic about the future of community banking. However, the percentage of respondents with a neutral or pessimistic outlook rose five points since last year.

This slight dip in optimism appears concentrated among smaller institutions under $1B in assets, which face stronger pressures from consolidation, tighter budgets and limited technology resources. Larger institutions remain almost universally confident, as they're better positioned to pursue acquisition opportunities and invest in technology modernization.

This growing gap reinforces the imperative to prioritize operational efficiency and targeted technology investments that deliver clear, measurable impact and make the most of the resources available.

I'm optimistic about the future of community banking.

52% Strongly Agree

34% Agree

13% Neither Agree nor Disagree

1% Disagree

Technology and Efficiencies

Efficient processes and modern technologies remain essential for growth and retention. An overwhelming 93% of respondents are interested in personalizing their offerings, and 74% think their processes could be more efficient. The latter represents a 15-point decrease from last year, suggesting that institutions may be feeling early effects of recent technology investments, including AI and automation.

My institution is interested in customizing our product offerings through technology integrations.

54% Strongly Agree

39% Agree

6% Neither Agree nor Disagree

1% Disagree

My institution's processes could be more efficient.

38% Strongly Agree

36% Agree

18% Neither Agree nor Disagree

7% Disagree

Growth and Engagement

With similar numbers to 2025, growth and digital engagement remain priorities for community financial institutions. More than eight out of 10 report attracting younger account holders, a positive sign as more of Gen Z enter the workforce.

However, while most respondents believe they're gaining traction with Gen Z and millennials, this sentiment contrasts with industry research. The Harris Poll found in 2024 that 79% of Gen Z (and 69% of Millennials) still consider a large national bank their primary financial institution.[1]

Simultaneously, though, the same poll pointed to a potential advantage for community financial institutions: Gen Z and Millennials reported the least satisfaction with their primary institution (mostly national banks) and the most openness to switching to a community bank or credit union.

Winning these accounts requires frictionless digital experiences, clearer market differentiation and timely, personalized touchpoints that reinforce engagement early and often throughout the account lifecycle.

My institution is growing its existing customer base.

54% Strongly Agree

38% Agree

7% Neither Agree nor Disagree

1% Disagree

My institution's customers are engaged on digital channels.

53% Strongly Agree

37% Agree

9% Neither Agree nor Disagree

1% Disagree

My institution is focused on increasing retail deposits.

45% Strongly Agree

37% Agree

17% Neither Agree nor Disagree

1% Disagree

My institution is attracting younger generations of account holders (e.g., Gen Z).

44% Strongly Agree

38% Agree

14% Neither Agree nor Disagree

1% Disagree

The Future of Branches

91% of respondents believe the branch will remain relevant for at least the next 10 years, up from 86% last year. This rising confidence (despite the popularity of mobile banking) points to a key advantage for community banks and credit unions. While national banks maintain large branch networks, local institutions often stand out in how branches operate: faster access to decision-makers, more personalized support and a relationship-driven approach that is difficult for larger institutions to replicate. Local branches remain a place of reassurance for account holders, offering the opportunity to resolve complex issues in person. Even tech-savvy Millennials and Gen Zers still value having the option to meet face-to-face when needed.

The branch experience is especially important in commercial banking. Commercial clients often rely on in-person conversations to navigate more complex or time-sensitive needs that benefit from direct expertise and faster decision-making. As community financial institutions pursue larger commercial portfolios, a high-quality and accessible branch relationship will become an even greater competitive advantage.

Our survey results suggest that more financial institution leaders are recognizing the need to balance branch and digital experiences. During the pandemic, this balance shifted heavily toward digital; today, it is returning toward the mean. Community financial institutions should intentionally manage the balance between branch and digital experiences, designing strategies that complement one another: seamless digital for routine needs and high-value, personal interactions at the branch for moments where expertise and trust matter most. Doing so requires clear performance metrics and accountability across both channels to ensure neither experience lags behind account holder expectations.

The branch will remain relevant for the next 10 years.

58% Strongly Agree

33% Agree

8% Neither Agree nor Disagree

2% Disagree

Key Highlights and Preview

The 2026 survey covered new and continuing trends, challenges and opportunities that community institutions face.

Key findings reveal three major areas of focus and concern: modernization, cybersecurity and efficiency through AI and automation.

Cautious Optimism Sets the Tone

Respondents report optimism about the future of their financial institutions, while acknowledging the challenges ahead.

- 52% are strongly optimistic about the future of community banking, and another 34% are optimistic.

AI and Automation Dominate Technology Plans

AI and automation are expected to have the largest impact on the financial industry again in 2026 and remain the top technology priority for respondents.

- Implementing efficiency drivers like automation and AI was the top 2026 technology priority, though AI regulatory concerns also persist.
- 85% agree that institutions adopting AI will gain a significant competitive advantage.
- Banks are nearly twice as likely as credit unions to believe that AI can enhance back-office efficiency, with 38% of banks recognizing its potential compared to just 21% of credit unions.

Strategic Modernization is Underway

Financial institutions view technology modernization as a foundational priority for 2026, reflecting a broader need to strengthen systems, improve integration and support future digital initiatives. While automation and AI are part of this landscape, modernization encompasses a wide range of efforts, from core and infrastructure improvements to enhanced data management and more flexible, connected platforms.

- 69% of institutions are extremely or somewhat likely to remain with their current provider at the next contract renewal, suggesting that institutions are seeking stability in their vendor relationships even as they plan for continued modernization.

Cybersecurity Remains a Top Concern

Cyber threats mount, placing greater pressure on institutions to stay ahead of bad actors.

- 83% of respondents feel well-prepared to respond to a cyberattack, though there is a gap in preparedness between community banks (85%) and credit unions (72%).

$5.56M is the average cost of a data breach in the financial industry, down from $6.08 million in 2024.[2]

Payments Influence Digital Engagement

Payments are emerging as a highly visible digital experience shaping account holder expectations in 2026. Community banks and credit unions are prioritizing cohesive, digital-first payment experiences that influence engagement, provider choice and growth across both consumer and business segments.

- 30% of respondents named improving payments as a top priority for growing digital engagement, second only to personalization and targeted marketing (31%).

Top Issues on Leaders' Minds

We asked respondents to pinpoint the issue they expect to matter most in 2026. Their answers shed light on the pressures they anticipate.

Artificial Intelligence

27%

AI has the potential to influence nearly every facet of banking, so it's not surprising that it leads as the top issue for 27% of respondents. Leaders increasingly view AI through a dual lens: to drive efficiency, speed and scale across operations, and as a force that accelerates fraud, scams and other forms of disruption. As institutions explore use cases, strong governance frameworks and clear policies are essential to guide responsible and effective adoption.

Cybersecurity/Data Privacy

16%

Although cyber threats and data privacy fell from last year's top spot, they remain a critical concern. As technology and AI advance, cybercriminals continue to develop more sophisticated techniques, increasing the need for investment in prevention and incident response capabilities.

Macroeconomic Pressures

10%

2025 saw rising tariffs and trade policy uncertainty drive up consumer prices and caused many businesses to pause investments and imports. The ripple effects could create new credit risks for community banks and credit unions in 2026.

Interest Rates

9%

About one-tenth of respondents are most concerned about how lower interest rates and a flatter yield curve will affect margins and their growth plans.

"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

Four categories each scored 8% of the vote.

Political Climate

The 43-day federal government shutdown at the end of 2025 highlights how political uncertainty can stall programs, raise credit stress and slow loan growth.

Payments Disruption

Respondents worry that the rapid growth of Buy Now, Pay Later (BNPL), digital wallets and other emerging payment methods will chip away at deposit balances, interchange revenue and account holder loyalty, as faster and more automated payment experiences make it easier for customers to move money outside their current primary banking relationship.

Non-Traditional Competition (e.g., Fintechs)

Fintechs are moving faster, increasing engagement and eroding traditional bank and credit union market share, across both retail and commercial segments. Their agility and digital strengths present a formidable competitive challenge not only among younger consumers but also as new players target business relationships with streamlined, digital-first offerings.

Fraud

Fraud continues to grow in scale and sophistication. More than 50%[3] of fraud executives believe fraud losses in U.S. banking payments will rise more than 10% in the next three years, and 68% expect AI use[4] by fraudsters to significantly increase in the next five years.

Rounding out the list were Regulatory Change (3%), Recruiting/Retaining Employees (1%) and Mergers & Acquisitions (1%).

Technology Trends in 2026

To stay competitive, financial institutions need to stay informed and proactive in their approach to emerging technologies. AI grabbed headlines and the top survey spot, but respondents also identified several other trends they expect to shape 2026.

Artificial Intelligence (AI)

50%

AI was named the most significant technology trend for the third consecutive year. Up 17 percentage points from 2025, AI is increasingly top of mind for executives as they explore ways to transform operations, drive efficiency, fight fraud and sharpen decision-making.

Digital Assets (e.g., Stablecoins, Tokenized Deposits, Cryptocurrencies)

20%

With one-fifth of the vote, digital assets are the second-largest tech trend for 2026. Tokenized deposits and stablecoins are emerging areas that institutions are monitoring closely as regulatory frameworks take shape.

Stablecoins are digital currencies designed to maintain a stable value, typically by being pegged to traditional assets like the U.S. dollar. They are increasingly discussed as potential alternatives for certain payment and settlement use cases.

By contrast, tokenized deposits are traditional bank deposits represented in digital form, allowing them to move and settle more efficiently while remaining within the regulated banking system.

Digital Transformation

11%

Digital transformation will remain a top focus, underscoring the need for streamlined digital channels that create stronger account holder experiences.

Real-Time Fraud Detection

8%

The emergence of AI and digital assets may help explain shifts in emphasis across technology priorities, but the importance of real-time fraud detection shouldn't be underestimated. Faster payments and more sophisticated attacks will continue to elevate the need for advanced monitoring and response.

Instant Payments

6%

Since its 2023 launch, the Federal Reserve's FedNow service has expanded rapidly, from 331 participating institutions to over 1,500. Adoption continues to accelerate as demand for faster, always-on payments grows.[3]

APIs/Open Banking

5%

While interest dropped sharply from last year's 11% result, APIs and open banking still offer financial institutions major opportunities, from automated workflows to fully integrated digital platforms.

Industry Insight

Stablecoins and tokenization are drawing heightened attention across the industry, even though the regulatory landscape is still taking shape. At the end of 2025, the FDIC published its first rules for the recently passed Guiding and Establishing National Innovation for U.S. Stablecoins (GENIUS) Act[4]. This could create opportunities over time as use cases develop, though most near-term applications remain limited, primarily in cross-border transactions. Any strategic engagement will require careful analysis and strong compliance frameworks.

Expert Perspective

Several CSI experts note that the novelty and visibility of AI may be overshadowing areas of more urgent operational concern to community financial institutions. This imbalance can leave institutions exposed if they direct disproportionate attention to AI exploration while underinvesting in risks that already affect daily operations.

At the same time, experts caution against accelerating AI initiatives without the governance structures needed to manage them. Without clear regulatory guidance and with real risks of biased or inconsistent outputs, institutions should prioritize governance, controls and policy frameworks before pushing new AI projects forward. Institutions should also take care to fully understand the risks and workload required for implementation, which they may understate or not fully grasp.

Fraud appears to rank lower in the survey than its day-to-day operational impact would suggest. Community financial institutions are seeing more impersonation schemes, relationship-based attacks and misuse of tools like ATM limits. Experts recommend evolving fraud strategies now, especially as instant payments scale and new NACHA rules go into effect in April 2026. They also note that the survey audience mix may have pushed fraud lower on the list, even though it remains top of mind for operations and security teams.

Payments disruption and digital assets may also be receiving less emphasis than their potential impact warrants. With interest in stablecoins rising, tokenized deposit models emerging and real-time payment rails expanding, experts caution that shifts in how money moves could affect liquidity, deposits and competitive dynamics more quickly than many institutions anticipate. Experts noted that instant and real-time payment capabilities, in particular, are becoming a baseline expectation for many business customers, increasing competitive pressure on institutions that cannot support faster, always-on money movement. As with fraud, the attention surrounding AI may be obscuring the scale and urgency of these developments.

The general sentiment on digital assets is mixed, however, and depends on the time horizon. Some CSI experts noted that stablecoins could pose a long-term threat to traditional fee-driven payment and transaction revenue, particularly if more money movement shifts outside the banking system. Others emphasized that near-term interest is often board-driven and exploratory, with today's most practical use cases remaining limited, mostly in cross-border transactions.

Our experts' guidance for 2026 is clear: keep exploring new technologies, but don't lose sight of the foundational risks, revenue pressures and consumer protections that will shape the year ahead.

"Balancing technology, innovation and risk management will define success in banking 2026."

Source: Survey Participant

Technology in Commercial Banking

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

While technology is shaping how community financial institutions grow their commercial portfolios, it's also creating significant hurdles. Nearly half of survey respondents cite technology limitations or integration gaps as their biggest obstacle to commercial growth, alongside competition from non-traditional providers, regulatory pressures and credit risk. Meanwhile, technology like data analytics and real-time payments are being used to drive business account growth, streamline lending processes and improve service.

What are your institution's biggest obstacles to expanding your commercial portfolio?

49% — Technology Limitations or Integration Gaps

44% — Competition from Fintechs or Alternative Lenders

42% — Regulatory Uncertainty or Compliance Burdens

42% — Competition from Large National Institutions

41% — Credit Risk and Underwriting Standards

33% — Staffing or Expertise Constraints

31% — Distribution and Relationship Management Challenges

How does your institution plan to leverage technology to advance its commercial banking priorities?

50% Integrating Data Analytics and Commercial Client Insights

45% Improving Cash Flow Visibility and Forecasting for Business Clients

44% Expanding Real-Time Payments Capabilities (e.g., TCH, RTP, FedNow)

43% Streamlining Commercial Lending Workflows End-to-End

43% Expanding Digital Commercial and Treasury Services

40% Leveraging Data to Streamline Credit Access and Decisioning

33% Streamlining Payment Orchestration and Workflows

30% Expanding Merchant Acquiring and Receivables Capabilities

28% Enhancing International Payments (e.g., SWIFT)

▶ **Institution Variance:** Banks 30% | CUs 15%

Industry Insight

The data highlights a gap between institutions' commercial growth goals and the technology foundations needed to support them. Nearly half of respondents (49%) say technology limitations or integration gaps are the biggest barrier to growing commercial portfolios, a signal that many institutions are still constrained by legacy systems and fragmented tech stacks. For many institutions, these limitations are most visible in customer-facing capabilities that require speed, automation and real-time data exchange, such as real-time payments, which are increasingly critical to winning and retaining commercial relationships. Experts note that mergers and acquisitions—accelerating in recent years—can compound these challenges by introducing multiple systems, inconsistent data structures and operational inefficiencies.

Many integration gaps trace back to outdated core processing platforms that can't support modern, automated workflows, analytics or real-time payments. Institutions with flexible, open cores are better positioned to implement data-driven decision-making, automated lending workflows and advanced treasury services while still delivering their trademark personal service.

At the same time, not every institution can pursue a core conversion immediately. Many can address near-term constraints by modernizing digital banking platforms that integrate with existing cores, enabling improving front-end account holder experiences as a first step toward broader transformation. Ultimately, technology modernization should be seen as a strategy to enhance—not replace—human connections.

These themes are especially pronounced for mid-sized institutions ($500M–$4.9B), which were most likely to cite technology limitations as their top obstacle, while institutions over $5B more often pointed to regulatory burden and fintech competition as primary constraints.

Expert Perspective

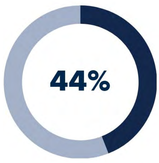
Technology challenges in commercial banking often stem from data silos and poor integration. Financial institutions may have access to vast amounts of information, but without connected systems, they struggle to gain full view of their commercial clients or extract actionable insights. Legacy platforms, combined with a growing and increasingly complex ecosystem of money movement, remain major bottlenecks.

Community banks and credit unions also face pressure to differentiate from larger competitors, and anticipating the needs of commercial clients is essential. Integrated tools and advanced data analytics can help position community institutions as an essential part of their business clients' financial operations. By unifying data across products and channels, institutions can better anticipate liquidity needs, identify cross-sell opportunities and flag early signs of risk, moving from reactive servicing to proactive engagement.

Institutions' Strategic Priorities

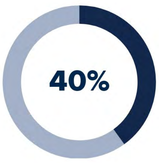
Strategic priorities give community financial institutions a clear focus on improving value and achieving long-term goals.

In 2026, technology modernization leads the way. Prioritization rises sharply with institution size, from 31% at smaller financial institutions ($100M–$250M) to 59% at larger ones ($5B–$10B). Cybersecurity and operational efficiency round out the top three, highlighting that institutions want technology and AI to improve multiple aspects of their operations.



Technology Modernization

▶ **Institution Variance:** Banks 47% | CUs 31%



Strengthening Cybersecurity

Increasing Operational Efficiencies

The survey also reveals several other areas of focus following closely behind:

25%
Market Expansion
▶ **Institution Variance:** Banks 22% | CUs 38%

19%
Customer Support Improvements

19%
Customer Financial Wellness/Inclusion

17%
Expanding Consumer Deposits

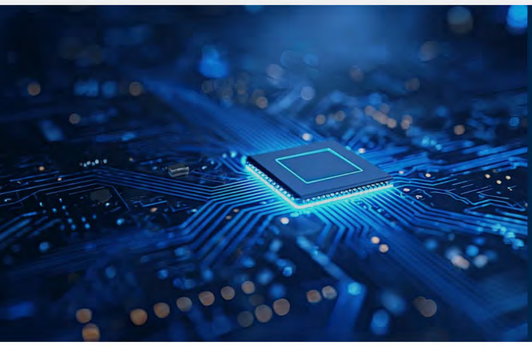
16%
Expanding Commercial Deposits

16%
Expanding Commercial Payment Services

15%
Opening New Branches

15%
Mergers & Acquisitions Activity

13%
Commercial Loan Growth
▶ **Institution Variance:** Banks 10% | CUs 31%



Industry Insight

Tech modernization is the gateway to nearly every other strategic priority. Simplifying platforms and processes frees up IT resources for transformational investments, while integrated, cloud-native systems let institutions leverage data analytics and AI effectively. Just as importantly, modernization enables the seamless, intuitive experiences account holders now expect. These capabilities support both deposit growth on the retail side and stronger commercial client relationships.

Without modern platforms in place, institutions struggle to integrate with APIs, automate workflows or extract useful insights from their data. Financial institutions that are built on a sturdy base will be better positioned to use technology strategically, not just operationally.

Expert Perspective

Respondents' top priorities—technology modernization, cybersecurity and operational efficiency—reflect a focus on strengthening the operational foundations that support long-term growth. These priorities are deeply interconnected: meaningful efficiency gains and secure digital experiences depend on having modern, flexible systems, clean data and integrated workflows.

While traditional growth levers like lending, branch expansion and M&A rank lower as standalone priorities, this does not signal a deprioritization of growth itself. Rather, it suggests that many institutions view technology modernization and operational readiness as table stakes for competing effectively, both to earn retail relationships and to support and retain a growing commercial portfolio.

Experts emphasize that "technology modernization" encompasses a wide range of efforts depending on an institution's size and infrastructure—from core and digital platform upgrades to network, hardware, analytics and cloud improvements. This variation underscores the importance of tailoring modernization strategies to each institution's starting point.

Our experts also noted that many institutions still approach technology as a series of features to implement, rather than a holistic architecture. This makes it difficult for institutions to identify the specific workflows, data connections or process changes needed to achieve the efficiencies they're targeting. When digital investments are layered on without strong integration, clear data flows and aligned workflows, they risk improving surface experience without meaningfully improving how the institution operates or scales.

This reinforces the need for a broader mindset shift. Community institutions increasingly need to think and act like technology companies: prioritizing architecture, integration and data readiness as the foundation for meaningful modernization.

Artificial Intelligence (AI)

AI is increasingly viewed as a practical tool for driving value, even as many institutions continue to balance its potential with important questions around governance, risk and customer perception. Community banks and credit unions have greater confidence and clarity about where AI could make an impact: automating routine tasks, strengthening security and freeing staff to focus on relationship-driven work.

The power and potential of AI is not lost on respondents, reflected by consistent responses across all asset sizes. Larger institutions report higher familiarity: 97% of institutions holding $5B–$10B in assets agree or strongly agree that they understand what AI is and how it can be applied in banking.

85%
Institutions that adopt AI will have a significant competitive advantage.

85%
Understand what artificial intelligence is and how it can be used in banking.

79%
Are optimistic about the potential of AI in banking.

When asked how AI could help their financial institution, the most-chosen benefits were:

57%
Cybersecurity

55%
Advanced Data Analytics

48%
Financial Crimes Prevention (e.g., Fraud, AML)

48%
Customer Service

46%
Customer Engagement (e.g., Chatbots, Virtual Assistants)

36%
Back Office Operations Efficiency
▶ **Institution Variance:** Banks 38% | CUs 21%

35%
Account Opening and Onboarding

34%
Lending Automation

34%
Personalized Marketing and Product Recommendations

Despite excitement and optimism surrounding AI, it also raises important questions for many respondents:

78%
AI should augment, not replace, human judgment in banking.

76%
Trust AI-driven decisions and outputs in banking.
▶ **Institution Variance:** Banks 78% | CUs 59%

62%
Are concerned about how customers will perceive the use of AI in banking.

56%
Believe AI poses regulatory/compliance risks for financial institutions.

50%
Are concerned about the potential of AI in banking.

- This is a substantial decrease from last year, when 83% reported concern.

Industry Insight

Recent global research from IBM and the Ponemon Institute reveals that AI adoption is outpacing security and governance. Nearly all (97%) organizations reported experiencing an AI-related security incident, often tied to insufficient access controls. 63% had no AI governance policies to manage AI or prevent the rise of shadow AI.[7]

The takeaway is clear: move quickly but govern carefully. AI deployed without proper controls and oversight policies raises the risks of data disclosures and unchecked shadow AI.

Shadow AI is the use of AI tools or applications by employees or end users without formal approval or oversight from the IT or governance teams. These unsanctioned activities can create security, compliance and operational risks for an institution.

Expert Perspective

AI offers real value in data-heavy areas like fraud prevention and security, but it's not magic. Effective use still requires careful, unbiased training, intentional implementation and ongoing oversight. Adoption alone doesn't guarantee results; its impact depends on how it's used and how well it's integrated into daily operations.

Strong governance is essential, especially in the absence of regulatory clarity, because AI systems can interact with sensitive data across the institution and introduce new risks if not properly controlled. Rather than broad access, effective governance ensures AI systems use the right data for the right purposes, with clear restrictions and continuous monitoring to prevent bias, unfair outcomes or blind spots. Community banks and credit unions should also weigh build-versus-buy decisions carefully and resist the temptation to chase "flashy" tools that distract from core priorities.

When implemented thoughtfully, AI can increase efficiency and deliver measurable value while keeping risk in check.

"AI is the best and worst thing for our current banking environment."

Source: Survey Participant

Top Technology Investments

Community financial institutions will continue to invest in tools that make banking faster, easier and more connected for their account holders.

Efficiency technologies like automation and AI continue to lead investment plans, but institutions are also prioritizing improving digital engagement, streamlining lending and connecting systems through open banking. Payments are evolving quickly, too, with growing interest in real-time options.

Explore what community financial institution leaders say will matter most in 2026.

Institutions' Top Technology Priorities

Read more

Advancing Digital Engagement

Read more

Open Banking

Read more

Automation in Lending

Read more

Payment Priorities and Trends

Read more

Cybersecurity

As digital innovation accelerates, financial institutions face an increasingly complex cyber landscape. AI-driven threats, evolving regulatory requirements and the rapid pace of technology are reshaping the risks institutions must manage.

This year's survey explored not only the cyber risks community institutions see on the horizon, but also their perceptions of institutional readiness, compliance practices, board oversight and budget priorities. The results show strong awareness of emerging risks (especially those fueled by AI) while also revealing areas where institutions may still underestimate vulnerabilities.

Cybersecurity Concerns on the Horizon

Read more

Institutions Assess Cybersecurity Readiness

Read more

Board-Level Cyber Oversight

Read more

Focus on Cybersecurity Compliance

Read more

Budgeting for Cybersecurity

Read more

Fighting Fraud on All Fronts

Fraud continues to rise and spread, driven in part by AI-powered scams that have become more sophisticated, convincing and easier to scale.

Our 2026 survey captures how these evolving threats are affecting institutions today and how confident respondents feel in stopping them.

Common Types of Fraud

Card fraud and check fraud remain the most frequently encountered forms of fraud, but several other types are affecting community banks and credit unions as well:

Over four in ten respondents encounter **card fraud (46%)** and **check fraud (42%)** the most at their financial institutions.

Closely behind were **phishing (32%), wire transfer fraud (31%), P2P fraud (27%)** and **fraudulent account opening (26%)**.

About two in 10 respondents reported **loan fraud (23%), ACH fraud (23%), account takeovers (22%)** and **synthetic ID fraud (21%)** as primary concerns.

Rounding out the list were **elder financial fraud (15%), insider threats (13%)** and **social engineering of staff (13%)**.

Synthetic Fraud on the Rise

An emerging type of identity fraud where a fraudster creates an entirely new persona by mixing real information with invented details. Often, a valid Social Security number is combined with a fabricated name, birth date or address. This mix of genuine and false data makes the identity look legitimate and helps it slip through verification checks.

Fraud Prevention Effectiveness

While respondents expressed concern about fraud, a majority feel their prevention measures are very or highly effective for all 13 types of fraud evaluated.

AI & Automation in Fraud Detection

To use AI effectively in fraud detection, institutions need clean, consistent and well-integrated data. These systems rely on well-defined red flags to identify fraudulent activity. A solid fraud program is essential before automating detection—without it, even advanced technologies can miss critical signals.

Leaders must also understand the security protocols and potential data usage associated with AI tools from third-party vendors, before committing to their adoption.

Read more in the Bank Director Intelligence Report, The Fraud Menace, sponsored by CSI.

Card and Check Fraud

Card and check fraud remain the most common types of fraud institutions face, and respondents express strong confidence in their ability to prevent them. Over eight in 10 feel their prevention measures for card and check fraud are highly or very effective.

Card Fraud Prevention Measures

41%
Highly Effective

41%
Very Effective

13%
Moderately Effective

3%
Slightly Effective

1%
Not Effective

Check Fraud Prevention Measures

46%
Highly Effective

41%
Very Effective

10%
Moderately Effective

2%
Slightly Effective

1%
Not Effective

AI and machine learning play an increasingly important role in card fraud prevention across the industry, enabling faster pattern recognition and risk scoring than traditional rules-based systems. These models can analyze large volumes of transaction data in real time to flag suspicious activity, while human oversight remains critical to account for nuance, avoid bias and ensure accuracy.

Check fraud has grown in recent years, even as check usage has declined overall. The Department of Treasury notes that paper checks remain easy targets because they display sensitive personal information and offer very little built-in security.[11]

ACH Fraud

Respondents ranked ACH as their third-strongest area of fraud prevention confidence.

ACH Fraud Prevention Measures

44%
Highly Effective

38%
Very Effective

14%
Moderately Effective

2%
Slightly Effective

2%
Not Applicable

Even with strong confidence in stopping ACH fraud, the system itself still poses risks. Most ACH payments settle the next day, and same-day ACH has transaction limits, giving fraudsters time to act before alerts go off. Because ACH is designed for efficiency and trust and not real-time security, delayed processing and limited oversight allow this type of fraud to persist.

Phishing

Phishing ranked as a top concern but near the bottom in prevention confidence, reflecting how difficult it is to stop attacks that target customers and employees through channels outside the institution's direct control.

Phishing Prevention Measures

35%
Highly Effective

34%
Very Effective

25%
Moderately Effective

3%
Slightly Effective

1%
Not Effective

2%
Not Applicable

Phishing remains the most-reported cybercrime, contributing to massive losses, but AI significantly increases the danger. Microsoft's 2025 Digital Defense Report found that AI-generated phishing emails have a 54% click-through rate, compared to just 12% for traditional phishing scams. According to Microsoft's analysis, this could make phishing up to 50+ more profitable, as well as much more costly for financial institutions.[12]

Account Takeover Fraud

Though respondents feel fairly confident in preventing account takeovers, Suspicious Activity Reports tied to this fraud have tripled in the last five years, indicating a growing threat.[13] Online marketplaces now sell phishing kits and stolen bank account credentials, making it easy for even low-skill criminals to launch attacks and profit at scale.

Account Takeover Prevention Measures

43%
Highly Effective

37%
Very Effective

17%
Moderately Effective

2%
Slightly Effective

2%
Not Applicable

Industry Insight

More convenient banking also means more opportunities for fraud. Tap-to-pay, embedded payments and one-click checkouts make transactions faster and more frictionless, but just as they remove barriers for customers, they remove barriers for fraudsters as well. Though adding some friction to digital processes may slow down the experience, it's crucial for protecting consumers and reducing fraud. If you aren't hearing complaints, you may not have enough safeguards in place.

Now, AI is raising the stakes. Tools like FraudGPT, BlackmailerV3 and ElevenLabs allow criminals to create believable, large-scale scams without the ethical limits of public AI systems. As fraud becomes easier to automate, financial institutions face growing pressure to balance speed, convenience and security without adding more risk for their account holders.

Expert Perspective

AI is making every type of fraud easier. To stay secure, financial institutions need tighter data integration, clearer insight into their vendor tools and to truly know their account holders.

Siloed data is a significant concern. When systems can't "talk" to each other, it's harder to spot patterns across channels and stop fraud quickly. Synthetic ID fraud is also growing as criminals blend real and fake personal details to create "new" account holders that slip through weak identity checks.

Regulatory uncertainty is another concern. With multiple AML Act components paused or rolled back, including the IA AML Rule, financial institutions still need to stay alert as most fraud ultimately flows through weak AML controls.[14] Participating in the FinCEN 314(b) communications network can strengthen AML efforts and potentially help avoid losses tied to suspicious transactions.

And as always, financial institutions that proactively educate account holders about scams can mitigate risk while building trust and loyalty.

Experts also noted that high self-reported confidence in fraud prevention often reflects perception rather than preparation. Several described a pattern of "wishful thinking," where institutions feel effective despite rising fraud losses and increasingly sophisticated attacks. This gap reinforces the need for deeper assessment, stronger controls and more integrated data across channels.

Top Regulatory Concerns

With AI and cybersecurity topping the list of Issues on Leaders' Minds, it's no surprise that the regulatory landscape around these topics is also front and center.

Respondents noted they are very or highly concerned in these compliance areas:

59%
Cybersecurity Compliance

58%
AI Governance

57%
Financial Crimes Compliance (e.g., AI, Analytics, Fraud Detection, BSA/AML Modernization)

55%
Managing Regulatory Change and Risk

53%
Cloud-Based Banking Technologies

53%
Digital Assets (e.g., Stablecoins, Tokenized Deposits, Cryptocurrencies)

50%
Building Your Financial Services Ecosystem (e.g., Fintech/Big Tech Partnerships, Third-Party Risk Management, Open Banking)

Four out of 10 respondents also reported concern about: Monetizing Data, UDAAP, Fair Lending, Housing Finance Reform and CFPB's Rule 1033 on Open Banking. Credit unions ranked Monetizing Data much higher than banks (64% vs 45%), a hesitation that could affect many areas of growth.

Cybersecurity Compliance

59%
Highly Concerned or Very Concerned

Cybersecurity remains the top regulatory concern for respondents. Mitigation measures like regular security assessments and multi-factor authentication can give banks and credit unions the tools they need to reduce risk and maintain trust with account holders.

35% Highly Concerned
24% Very Concerned
22% Moderately Concerned
10% Slightly Concerned
9% Least Concerned

AI Governance

58%
Highly Concerned or Very Concerned

AI governance is the second biggest regulatory worry for respondents, and with good reason: a recent U.S. Government Accountability Office report highlighted AI risks, including biased lending decisions, data quality issues, privacy concerns and new cybersecurity threats.[25] The OCC has issued guidance recommending transparency, accountability and strong risk management for AI systems[26], while the NCUA launched a formal AI compliance plan to help credit unions use AI safely.[27]

24% Highly Concerned
34% Very Concerned
24% Moderately Concerned
10% Slightly Concerned
7% Least Concerned

Financial Crimes Compliance

(AI, Analytics, Fraud Detection, BSA/AML Modernization)

57%
Highly Concerned or Very Concerned

Financial crime compliance worries many respondents. FinCEN's proposed rule under the AML Act of 2020 would require all financial institutions to build "effective, risk-based and reasonably designed" AML/CFT programs.[28] Without clear guidance, institutions face uncertainty that can increase the risk of compliance gaps or costly penalties.

27% Highly Concerned
30% Very Concerned
23% Moderately Concerned
15% Slightly Concerned
3% Least Concerned

Managing Regulatory Change and Risk

55%
Highly Concerned or Very Concerned

Regulatory change is keeping institutions on their toes as rules continue to shift and evolve. For example, U.S. regulators recently proposed redefining "unsafe or unsound practices" and removing reputation risk from exam criteria, signaling a move toward more measurable, financial-based oversight.[29]

27% Highly Concerned
28% Very Concerned
24% Moderately Concerned
13% Slightly Concerned
8% Least Concerned

Cloud-Based Banking Technologies

53%
Highly Concerned or Very Concerned

Cloud-based banking technologies offer many benefits to scale and resilience, but regulators are pushing hard to ensure that institutions don't simply offload risk when they outsource to cloud providers. Financial institutions are expected to carefully negotiate contracts with cloud providers that include strong transparency and security provisions.

19% Highly Concerned
34% Very Concerned
23% Moderately Concerned
13% Slightly Concerned
10% Least Concerned

Digital Assets (e.g., Stablecoins, Tokenized Deposits, Cryptocurrencies)

53%
Highly Concerned or Very Concerned

2025 saw regulatory shifts giving financial institutions more room to engage with crypto—but with higher expectations. The FDIC and OCC both rolled back earlier restrictions, now allowing activities like crypto custody and participation in blockchain networks as long as financial institutions can demonstrate strong risk management.[30] [31] With Congress advancing the GENIUS Act to create a clearer framework for payment stablecoins, institutions can expect both new opportunities and closer scrutiny ahead.[32]

22% Highly Concerned
31% Very Concerned
28% Moderately Concerned
13% Slightly Concerned
6% Least Concerned

Industry Insight

Banks and credit unions are navigating rising regulatory pressure in many areas, including cybersecurity and AI governance. At the same time, recent remarks from OCC and Federal Reserve officials encourage community banks to embrace digital assets and technology to stay competitive.[33] Regulators are signaling expectations for stronger controls and continued innovation, creating pressure for institutions to advance on both fronts.

Expert Perspective

With the FFIEC's Cybersecurity Assessment Tool (CAT) retirement in August 2025, experts see a growing gap between regulatory expectations and institutional readiness.[34] Many institutions feel uncertain about what "good enough" looks like for AI and cybersecurity governance or evolving BSA/AML requirements.

To mitigate risk, compliance teams need a deeper understanding of how AI-enabled threats, fraud and cloud dependencies change their risk profile and how regulators expect those risks to be documented and addressed.

The Future of Community Banking

Community banks and credit unions are navigating an environment where competitive, technological and regulatory pressures are intensifying. Fintech expansion, megabank competition, rising fraud and widening technology gaps have created conditions that are challenging enough to feel existential for many institutions. Yet the 2026 survey reflects an industry that understands the stakes and is preparing to meet them.

To remain indispensable in consumers' increasingly digital financial lives, community institutions must evolve from reactive transaction processing to more proactive, insight-driven service. Brand loyalty can no longer be assumed. Meeting rising expectations increasingly depends on modernization and integration efforts that support automation, actionable insights and, over time, more scalable personalization.

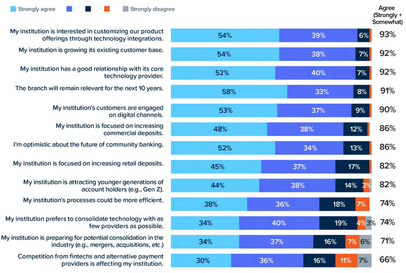
The survey results suggest that many institutions recognize this shift and are aligning their priorities accordingly. As they look ahead to 2026, community financial institutions appear ready to move forward with cautious optimism. Their responses point to a clear focus on strengthening the foundational capabilities needed for sustained transformation. When paired with the relationship-centered service that has always defined community banking, these investments position institutions not just to adapt, but to compete.

Community banks and credit unions that blend modern digital capabilities with trusted, human-centered service will be well-positioned to remain essential financial partners to the retail and business account holders they serve, in 2026 and in the years ahead.

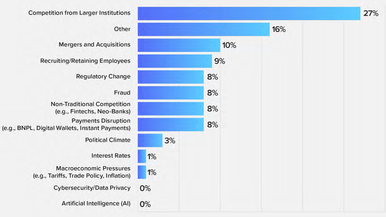
Appendix

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.

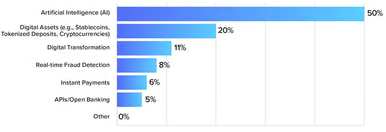
1: To what extent do you agree or disagree with the following statements?



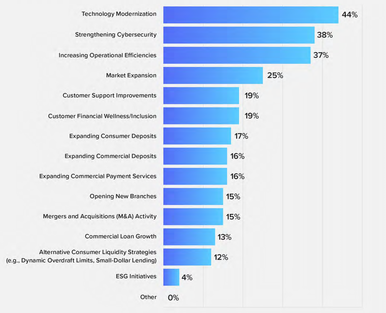
2: Which issue do you expect will most affect the financial industry in 2026?



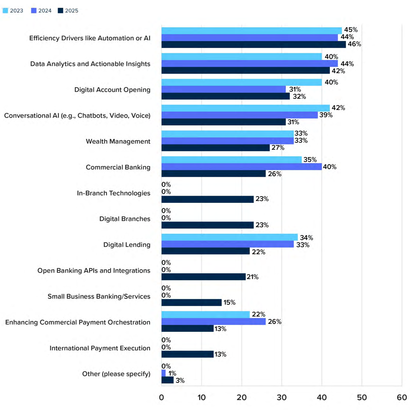
3: Which technology trend will most affect the financial industry in 2026?



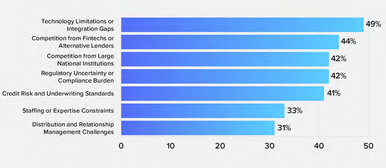
4: What are your institution's top 3 strategic priorities for 2026? Please select three options.



5: Which 3 technologies will your institution prioritize in 2026? Please select three options.

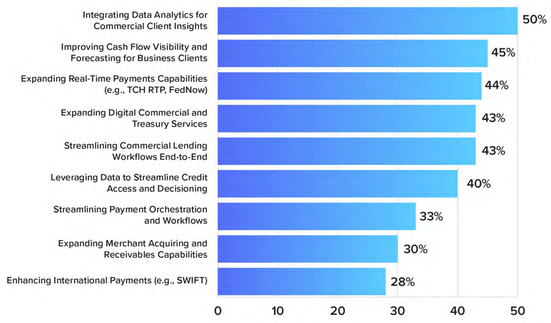


6: What are your institution's biggest obstacles to expanding your commercial portfolio?

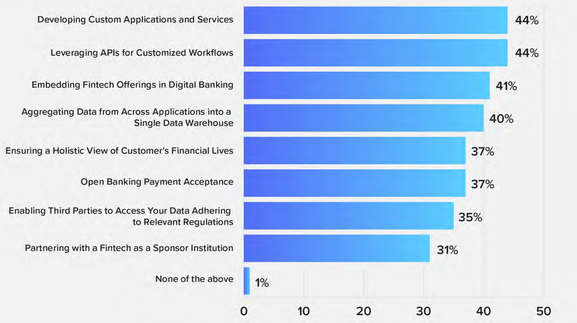


(continued on next page)

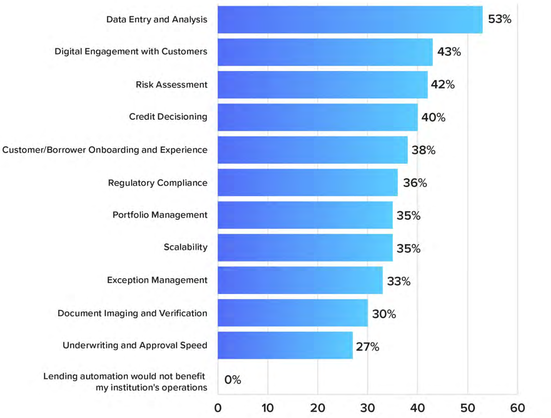
7: How does your institution plan to leverage technology to advance its commercial banking priorities?



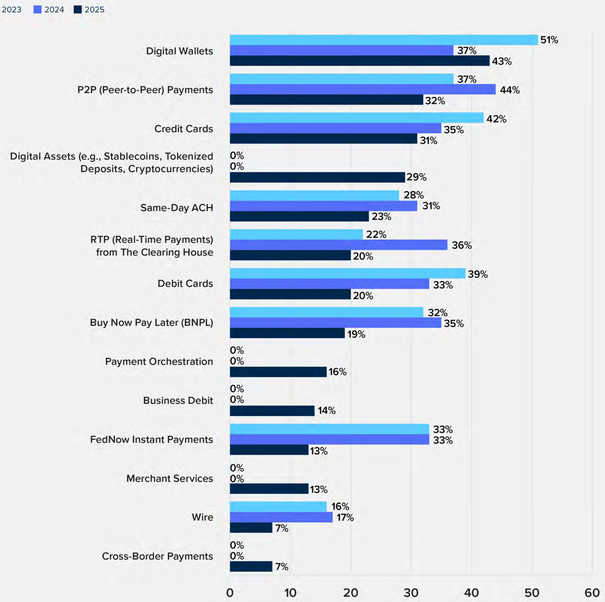
8: What are your institution's primary goals for implementing Open Banking APIs? Please select all that apply.



9: In what areas would lending automation benefit your institution's operations?

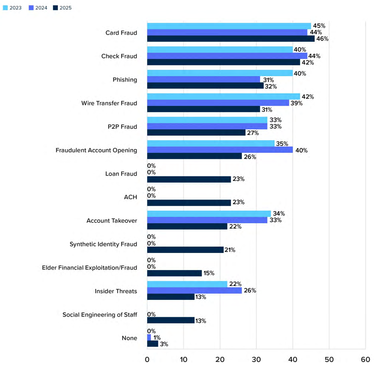


10: Which 3 payment technologies will your institution focus on in 2026? Please select three.

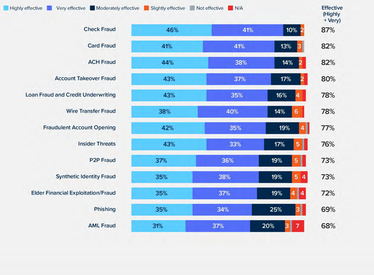


(continued on next page)

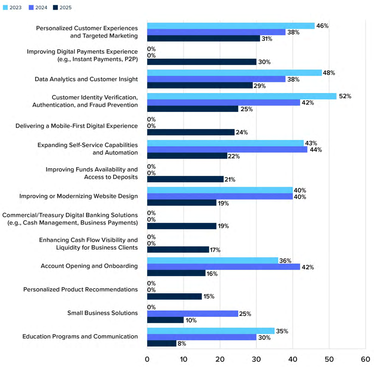
11: What are the most common types of fraud your institution encounters?



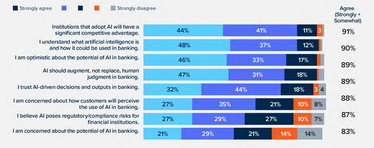
12: How effective are your current fraud prevention measures in mitigating the following risks?



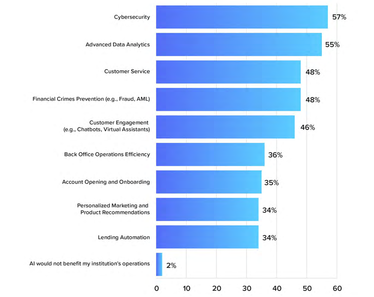
13: What are your top 3 priorities for enhancing digital customer engagement in 2026?



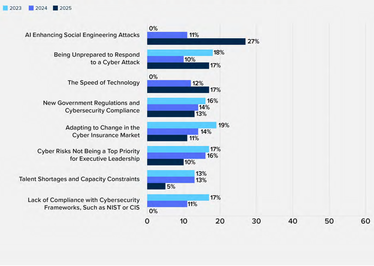
14: To what extent do you agree with the following statements?



15: In what areas would artificial intelligence (AI) benefit your institution's operations?



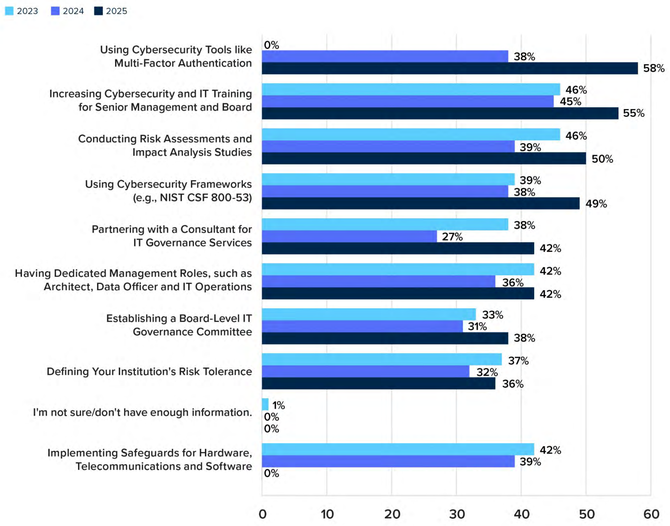
16: What is your greatest forward-looking cybersecurity concern?



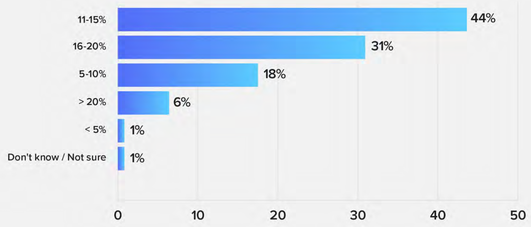
17: For each statement, mark whether you agree or disagree.

(continued on next page)

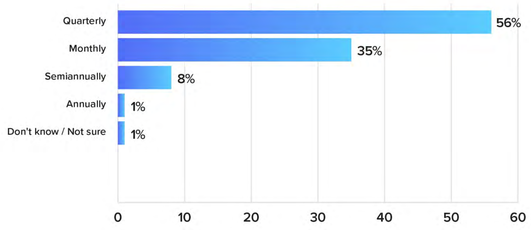
18: What tools and resources does your institution use to ensure cybersecurity compliance?



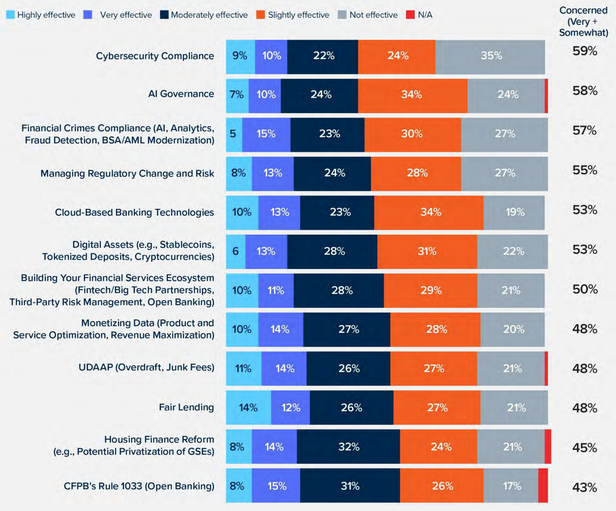
19: What percentage of your annual IT budget is dedicated to cybersecurity?



20: How often does your institution's leadership present cybersecurity updates to your board of directors?



21: Please rate your level of concern for the following regulatory issues. If you are not familiar with the regulatory issue, please select Don't Know.



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 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] Apiture, White Paper: Attracting Gen Z and Millennials

[2] IBM, Cost of a data breach 2025

[3] Datos Insights, Real-Time Payments: Three-Year Outlook and Sentiments From Fraud Executives

[4] Datos Insights, Five Forces Disrupting Global Fraud Prevention by 2030

[5] The Financial Brand, FedNow Reaches 1,500 Banks as Instant Payments Grow

[6] FDIC, FDIC's Hill expects first GENIUS Act rules by year-end

[7] IBM, Cost of a data breach 2025

[8] Reuters, US judge blocks consumer agency's 'open banking' rules for now

[9] GlobeNewswire, Digital Lending Growth Analysis and Outlook Report

[10] CFPB, Federal Regulators Issue Joint Statement on the Use of Alternative Data in Credit Underwriting

[11] Nacha, Same Day ACH Leads ACH Network Growth in Second Quarter

[12] The Clearing House, RTP-Q2-Value-Surge

[13] PaymentsJournal, FedNow Transaction Limit Will Match RTP at $10 Million

[14] BusinessWire, U.S. SMBs Say Payment Innovation Is Key Driver of Growth

[15] American Bankers Association, Fall 2025 Morning Consult Survey Results Consumer Satisfaction

[16] ISC2, Results of the 2024 ISC2 Cybersecurity Workforce Study

[17] PYMNTS, Financial Services 'Most Breached Industry' Amid Data Leak Surge

[18] NACD, 2023 Director's Handbook on Cyber-Risk Oversight

[19] ABA Banking Journal, Inspector general report finds CFPB cybersecurity lacking

[20] Gartner, Gartner Forecasts Global Information Security Spending to Grow 15% in 2025

[21] Department of the Treasury, Request for Information on Potential Actions to Address Payments Fraud

[22] The Register, AI makes phishing 4.5x more effective, Microsoft says

[23] Forbes, Fraud In America 2025: The Consumer Threat Landscape

[24] U.S. Department of the Treasury, Treasury Announces Postponement and Reopening of Investment Adviser Rule

[25] GAO, GAO-25-107197, ARTIFICIAL INTELLIGENCE: Use and Oversight in Financial Services

[26] Office of the Comptroller of the Currency, Acting Comptroller Rodney E. Hood Pre-Recorded Remarks

[27] NCUA, NCUA Artificial Intelligence Compliance Plan

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

[29] JDSupra, US Banking Regulators Propose to Refocus Supervision on Material Risks

[30] FDIC, FDIC Clarifies Process for Banks to Engage in Crypto-Related Activities

[31] Office of the Comptroller of the Currency, OCC Clarifies Bank Authority to Engage in Certain Cryptocurrency Activities

[32] CSI, The GENIUS Act and Beyond: Strategic Implications for Community Banks

[33] American Banker, Fed's Bowman seeks level field for banks on digital assets

[34] CSI, Beyond the CAT: Building a Resilient IT & Cyber Governance Program in a Post-CAT Era

Institutions' Top Technology Priorities

Aside from a few outliers, top tech investments for 2026 are tightly clustered. This suggests that institutions are pursuing multiple innovation paths simultaneously rather than rallying around one clear priority.

For the third year in a row, efficiency drivers like automation and AI top respondents' list of technology priorities. In a close tie for second are data analytics and digital account opening.

37%
Efficiency Drivers like Automation or AI

31%
Data Analytics and Actionable Insights

31%
Digital Account Opening

25%
Conversational AI (e.g., Chatbots, Video, Voice)

24%
Wealth Management

Institutions with $5B-$10B in assets named conversational AI as a top priority, signaling a move into greater use of automation in customer service.

22%
Commercial Banking

22%
In-Branch Technologies

21%
Digital Branches

21%
Digital Lending
▶ **Institution Variance:** Banks 19% | CUs 31%

21%
Open Banking APIs and Integrations

Rounding out the responses were:

12%
Small Business Banking/Services
▶ **Institution Variance:** Banks 10% | CUs 21%

12%
Enhancing Commercial Payment Orchestration

11%
International Payment Execution

Industry Insight

Top technology priorities point to a shift in focus from mere adoption to stronger integration. The emphasis on automation, digital account opening and data analytics reflects a need to reduce manual effort, streamline workflows and address longstanding data and integration challenges.

Open banking plays an increasingly important role in that effort, giving institutions new ways to automate workflows, improve data consistency and reduce friction between systems. The challenge now will be connecting these technologies in ways that streamline operations and enhance the account holder experience, without losing the personalized service that differentiates community banking.

Expert Perspective

The clustering of so many priorities together signals that institutions are juggling multiple technology efforts at once. Unsurprisingly, efficiency-focused tools still lead as community institutions look for ways to do more with less. The continued focus on digital account opening suggests that even institutions with established solutions see opportunities to streamline onboarding and back-office processes, with open banking increasingly serving as an enabling layer that accelerates integration.

Conversational AI is gaining momentum, but many institutions are still searching for its most valuable use cases. Meanwhile, commercial and small business banking saw notable declines in prioritization this year, reflecting a focus on modernization and operational readiness in general.

Experts emphasized that the real differentiator ahead will be how prepared institutions are to use their data, both to support AI initiatives and strengthen decision-making. That readiness gap is significant. In recent research conducted by Cornerstone Advisors in partnership with Apiture, only 11% of bankers rated their institution's data strategy as very effective. Average scores across key data capability areas were around the midpoint of Cornerstone's scoring model, suggesting a gap between data availability and the ability to consistently use that data to drive outcomes.

Data analytics and actionable insights underlie most of the technology priorities identified in the survey, from personalization to automation to commercial growth. AI on its own is not a strategy; the value comes from how insights generated by AI are interpreted and applied, guided by clear questions and translated into concrete actions.

"Our organization as a whole is optimistic about the utilization of artificial intelligence in the future."

Source: Survey Participant

Return to main section

Automation in Lending

With loans being a primary source of revenue for many community banks and credit unions, lenders are looking to streamline and optimize processes wherever possible. From data entry to risk assessment, automation can improve efficiency and enhance the loan application experience.

We asked respondents to identify where their institutions would benefit from automation in lending. Although banks and credit unions prioritize certain benefits differently; both groups agree on the value of automating data management, digital engagement and credit decisioning.

53%
Data Entry and Analysis

43%
Digital Engagement with Borrowers

42%
Risk Assessment

40%
Credit Scoring and Decisioning

▶ **Institution Variance:** Banks 44% | CUs 23%

In addition to the top four, respondents also found other beneficial areas of lending automation:

38%
Borrower Onboarding & Experience

36%
Regulatory Compliance

35%
Scalability

35%
Portfolio Management

33%
Exception Management

30%
Document Imaging & Verification

▶ **Institution Variance:** Banks 28% | CUs 41%

27%
Underwriting & Approval Speed

▶ **Institution Variance:** Banks 30% | CUs 15%

Industry Insight

Automation helps community financial institutions speed up several aspects of the lending process, from data entry and analysis to improved credit decisioning, while reducing manual effort and operational bottlenecks.

Digital lending is projected to grow at a compound annual rate of 15.5% through 2034, driven by increasing adoption and demand for faster, paperless financial services.[9]

Expert Perspective

The use of alternative data (such as transaction histories and payment patterns) in credit scoring is on the rise. This practice, recommended by the five federal financial regulatory agencies since 2019, can provide a more accurate and inclusive view of a borrower's "creditworthiness" and ability to repay.[10]

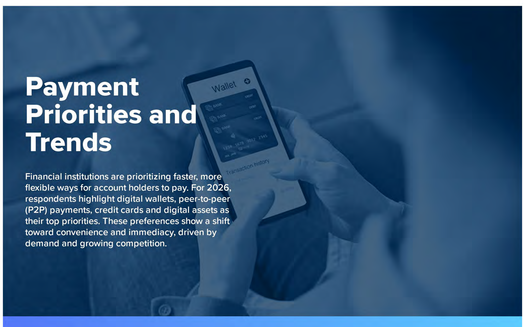
However, challenges remain. Our experts emphasize that AI models employed in lending automation must be trained carefully to avoid bias and maintain transparency for regulatory compliance. Smaller financial institutions often face hurdles related to platform integration, data access and the rising costs associated with implementing more advanced AI capabilities. Commercial lending, in particular, still relies heavily on manual credit review.

Targeted automation, often delivered through technology partners, can streamline processes such as risk assessment, financial spreading and ongoing credit monitoring. Community banks and credit unions that successfully address these challenges can improve efficiency, enhance account holder satisfaction and drive revenue growth.

"The banks that blend new tech with personal service will be the ones that stay ahead and keep customers loyal."

Source: Survey Participant

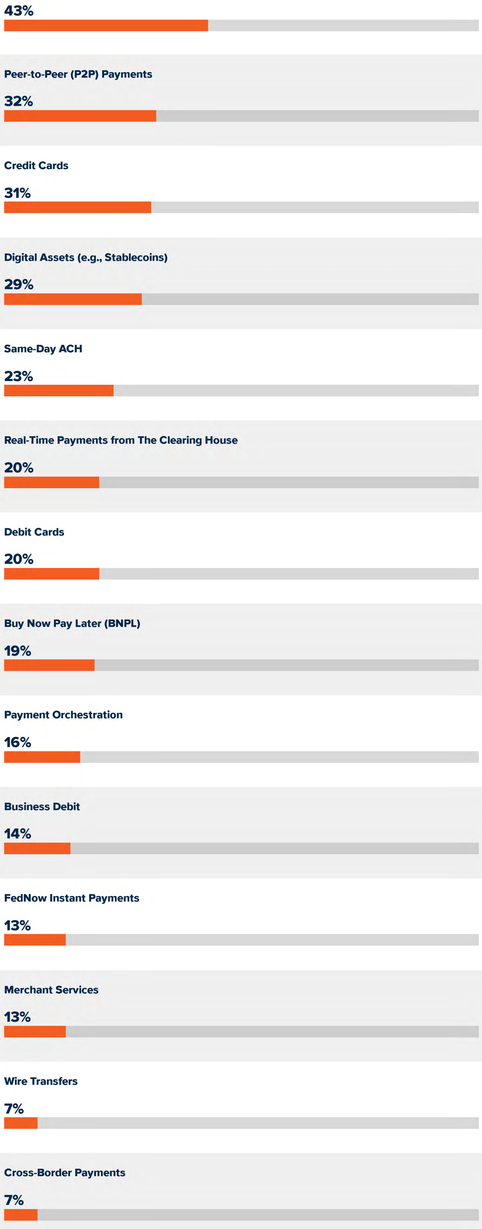
Return to main section



Payment Priorities and Trends

Financial institutions are prioritizing faster, more flexible ways for account holders to pay. For 2026, respondents highlight digital wallets, peer-to-peer (P2P) payments, credit cards and digital assets as their top priorities. These preferences show a shift toward convenience and immediacy, driven by demand and growing competition.

Respondents were asked to select their top three payment priorities for 2026.



Industry Insight

The prominence of digital wallets and peer-to-peer payments highlights growing demand for faster, more convenient ways to move money, particularly among consumers and small businesses that increasingly expect payments to be embedded seamlessly into their everyday financial activities.

Digital wallets allow users to store payment credentials and complete transactions quickly across channels, while peer-to-peer (P2P) payments enable fast, direct transfers between individuals and businesses. Together, these tools are reshaping expectations around speed, ease of use and accessibility in everyday payments.

U.S. payments continue accelerating toward real-time capabilities. Same-day ACH retains its momentum, reporting a 5% increase in transactions and a 7.9% increase in value year-over-year in Q2 2025.[17] Instant payments are rising even faster: The Clearing House's Real-Time Payments (RTP) network averaged 1.18 million daily payments in Q2 2025[18], while FedNow processed more than 2.1 million payments in the same quarter (up sharply from 1.3 million in Q1).[19]

This combined growth across Nacha, RTP and FedNow suggests continued progress toward the high levels of real-time payment adoption seen in markets such as the U.K., Brazil and India.

Expert Perspective

Experts agree that the real payments story in 2026 will be the shift toward a fully digital-first experience. Community banks and credit unions are prioritizing tools that let account holders manage spending, subscriptions, rewards and loyalty in one seamless place.

Small and medium-size businesses (SMBs) are driving much of this change. Nearly half (46%) of SMBs see value in instant or real-time payments, and 41% want "tap on phone" capabilities that turn mobile devices into contactless terminals.[20] AI is also gaining traction in payments applications, with 79% of SMBs citing its importance in fighting fraud. Experts noted that modern payment capabilities increasingly influence SMBs' choice of financial provider.

At the same time, other trends are shaping institutional strategy:

- Digital wallets and instant payment tools are becoming essential for staying competitive.
- Credit card usage remains strong, even as debit cards gradually decline.
- Payment orchestration and platform modernization are emerging as key levers to reduce friction and drive revenue.
- AI is playing a larger role in improving fraud scoring and tailoring offers based on transaction patterns.

Institutions are also watching emerging risks and opportunities, including stablecoins and tokenized deposits, which some worry could displace deposit revenue over time. And while real-time payment adoption varies across markets, the broader priority is clear: deliver a cohesive, secure and convenient payment experience that meets modern consumer and business expectations.

"AI and real-time payments will drive the next wave of innovation in finance."

Source: Survey Participant

Return to main section

Advancing Digital Engagement

Consumers and businesses alike expect seamless, consistent experiences across every part of their digital lives, and banking is no exception. Continuous and personal engagement will be essential.

For 2026, respondents identified their key priorities to strengthen digital engagement:

31%
Personalized Customer Experiences and Targeted Marketing

30%
Improving Digital Payments Experience (e.g., Instant Payments, P2P)

29%
Data Analytics and Customer Insight
▶ **Institution Variance:** Banks 31% | CUs 15%

Several other digital engagement priorities trailed the top three, including:

25%
Customer Identity Verification and Authentication
▶ **Institution Variance:** Banks 20% | CUs 54%

24%
Delivering a Mobile-First Digital Experience

22%
Expanding Self-Service Capabilities and Automation

21%
Improving Funds Availability and Access to Deposits

19%
Modernizing Website Design

19%
Commercial/Treasury Digital Banking Solutions (e.g., Cash Management...)

17%
Enhancing Cash Flow Visibility and Liquidity for Business Clients

16%
Account Opening and Onboarding
▶ **Institution Variance:** Banks 14% | CUs 31%

Industry Insight

Banks and credit unions have more data than ever, but much of it remains locked in silos, making personalization difficult. That disconnect is a significant challenge: institutions often struggle to translate rich account holder data into timely, relevant interactions that anticipate needs rather than simply respond to them.

This gap creates a clear opportunity for community banks and credit unions. When data integration and modern tools are combined with strong local relationships, institutions are better positioned to deliver more engaging, customized experiences than larger regional and national competitors.

Expert Perspective

Institutions' digital engagement priorities reflect a growing realization: community banks and credit unions have rich account holder data but struggle to use it to gain deeper insights and shape strategy. Having this information allows for a shift from managing transactions to managing *interactions*—understanding not only what account holders do, but *why they do it*.

Personalization through smarter segmentation and relevant recommendations drives real outcomes, including stronger onboarding, higher card usage, better digital engagement and lower churn. By connecting data across channels and using it to inform timely, relevant outreach, institutions can shift from reactive service to proactive engagement that further strengthens relationships and increases lifetime value.

"AI, automation and data-driven personalization are no longer optional—they're foundational to competitive banking in 2026."

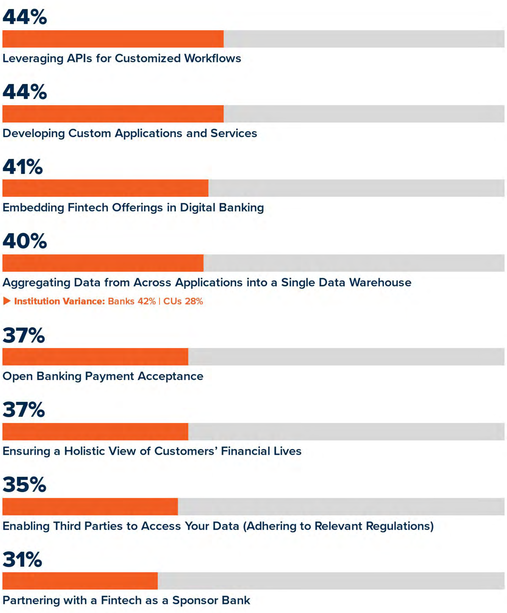
Source: Survey Participant

Return to main section

Open Banking

Open banking through APIs is giving financial institutions greater flexibility and choice in how they build and deliver services. By enabling systems to exchange data securely and consistently, open banking allows banks and credit unions to modernize and innovate with new capabilities, collaborate with integrated partners and streamline workflows.

When asked to select their open banking goals, respondents said that they are:



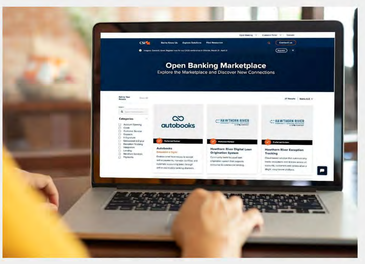
Industry Insight

Open banking adoption continues to grow as banks and credit unions seek to modernize operations and deliver more personalized digital services. Institutions are using open banking to work with fintech partners in multiple ways, including embedding fintech capabilities directly within their digital banking environments and participating in sponsorship banking arrangements. Across these models, institutions' strongest interest centers on embedding fintech capabilities directly into their digital banking environments.

In practice, however, sponsorship banking remains highly resource intensive, requiring continuous monitoring, compliance workflows and data transparency. Many small and midsize institutions underestimate this overhead until they are deep into these programs, especially when data is fragmented, and processes rely heavily on manual or file-based workflows. This operational reality may help explain why sponsorship banking ranks lower among stated priorities in this year's survey, even as institutions continue to explore other open banking use cases.

41% of respondents say embedding fintech capabilities into digital banking is a priority, reflecting a strong interest in delivering tightly integrated experiences within the bank's own digital environment. Taken together, these dynamics help explain why institutions are increasingly focused on stronger data integration and orchestration, often supported by open banking capabilities, to manage complexity and risk more effectively.

Regulatory uncertainty also persists: a federal judge recently paused enforcement of the Consumer Financial Protection Bureau (CFPB)'s open banking rule, leaving compliance timelines and requirements in flux.[8]



Expert Perspective

Open banking using flexible system-agnostic technology can deliver significant operational and account holder experience benefits by addressing growing needs, including expanding offerings through fintech partnerships, and enabling secure, transparent data sharing that gives customers greater control over their information. Instead of relying on a single provider, open banking lets financial institutions integrate these capabilities from multiple partnerships, choosing solutions that best meet their current and future needs, while maintaining strong oversight.

That said, realizing this value is not always straightforward. CSI experts observed that while institutions express strong interest in embedded fintech and API-enabled data sharing, many still operate across fragmented core, digital and data environments. This fragmentation can limit the ability to replace legacy data-sharing methods, provide a unified view of third-party connections, or act consistently on the insights gained from these integrations.

Open banking is most effective when treated as a foundational capability rather than a collection of isolated integrations. By focusing first on the outcomes they want to deliver—such as faster product expansion, greater transparency for account holders, or a more complete view of customers financial lives—institutions can guide integration priorities and build toward scalable, long-term modernization.

Return to main section

Cybersecurity Concerns on the Horizon

Community financial institutions see many cyber risks on the rise in 2026. AI-driven social engineering stands out as the leading concern, followed by concerns about cyberattack response and keeping pace with rapidly evolving technology.

Below are the cybersecurity concerns at the forefront of respondents' minds in 2026:

AI Enhancing Social Engineering Attacks

Being Unprepared to Respond to a Cyberattack

The Speed of Technology

New Government Relations and Cybersecurity Compliance

Adapting to Changes in the Cyber Insurance Market

Cyber Risks Not Being a Top Priority for Executive Leadership

Talent Shortages and Capacity Constraints

Industry Insight

AI-driven social engineering became the top concern for 2026 by a wide margin, jumping 16 percentage points from 2025. Generative AI now enables attackers to send more realistic phishing emails, deepfakes and voice impersonations. This is especially critical for financial institutions to address, given that U.S. adults trust banks the most to protect them from fraud (by a 6-to-1 margin over the next most-trusted entity).[15]

Notably, only 5% worry about talent shortages, despite a well-documented cybersecurity workforce gap[16]. This could be a potential blind spot heading into 2026.

Expert Perspective

Our experts highlight two fast-growing threats: voice cloning and QR code phishing.

Voice cloning tools can replicate someone's voice in minutes, letting attackers impersonate executives, employees or account holders. This makes verbal verification far less reliable.

QR code phishing is on the rise for similar reasons. Malicious QR codes, often disguised through color changes or split images, can be placed anywhere and send users' phones to harmful links that bypass traditional security controls.

Both threats show how AI is making attacks more personal and harder to detect, reinforcing the need for prevention, awareness and strong human-centered defenses.

"Cybersecurity is now a major concern for most financial institutions because digital payment systems are increasing day by day."

Source: Survey Participant

Return to main section

Board-Level Cyber Oversight

Over half of respondents indicate that their board of directors receives cybersecurity updates quarterly, while another one-third receives monthly updates. This frequency shows a strong emphasis on regular cybersecurity communication at the leadership level.

Cybersecurity Update Frequency

Industry Insight

Cyber threats have risen to their highest level yet. As of July, the U.S. was on track for a record number of data breaches in 2025, with financial services experiencing the highest incident rates.[17]

With that in mind, consistent and comprehensive cyber-risk reporting helps CISOs build board confidence. It gives board members an understanding of emerging threats so they can allocate appropriate resources and make informed decisions to protect the institution and its account holders. Regular reporting also reinforces cybersecurity as a core business priority, not just an IT issue.

Expert Perspective

Our experts were encouraged that 90% of institutions report cybersecurity updates to their boards monthly or quarterly, which aligns with governance best practices[18]. Anything less frequent risks falling short of proper oversight.

Depth and context in reporting matters just as much as frequency, however. Our experts recommend boards ask for trend data over time, as well as corresponding detection and mitigation rates. Point-in-time snapshots often fail to capture a full view of how threats and defenses are evolving over time.

Return to main section

Institutions Assess Cybersecurity Readiness

In addition to their cybersecurity concerns, respondents shared their perspectives on their own institution's cybersecurity readiness.

Respondents were asked to rate their level of agreement with seven readiness statements. Overall confidence was high, with over 80% of respondents agreeing or strongly agreeing with most statements, though credit unions often lagged about 10 percentage points behind banks. Their combined responses were as follows:

I clearly understand my institution's cyber risk.

88%

Agree (Strongly + Somewhat)

▶ Institution Variance: Banks 91% | CUs 79%

- **48%** Strongly Agree
- **40%** Somewhat Agree
- **10%** Somewhat Disagree
- **1%** Strongly Disagree

My institution has a trusted partner for cybersecurity.

87%

Agree (Strongly + Somewhat)

▶ Institution Variance: Banks 89% | CUs 77%

- **42%** Strongly Agree
- **45%** Somewhat Agree
- **13%** Somewhat Disagree
- **0%** Strongly Disagree

Our cybersecurity education program is effective.

86%

Agree (Strongly + Somewhat)

▶ Institution Variance: Banks 88% | CUs 74%

- **46%** Strongly Agree
- **40%** Somewhat Agree
- **13%** Somewhat Disagree
- **0%** Strongly Disagree

My institution is well prepared to respond to a cyberattack.

83%

Agree (Strongly + Somewhat)

▶ Institution Variance: Banks 85% | CUs 72%

- **44%** Strongly Agree
- **39%** Somewhat Agree
- **15%** Somewhat Disagree
- **1%** Strongly Disagree

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

82%

Agree (Strongly + Somewhat)

- **41%** Strongly Agree
- **41%** Somewhat Agree
- **15%** Somewhat Disagree
- **3%** Strongly Disagree

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

80%

Agree (Strongly + Somewhat)

- **38%** Strongly Agree
- **42%** Somewhat Agree
- **17%** Somewhat Disagree
- **2%** Strongly Disagree

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

73%

Agree (Strongly + Somewhat)

- **38%** Strongly Agree
- **35%** Somewhat Agree
- **19%** Somewhat Disagree
- **6%** Strongly Disagree

Industry Insight

Credit unions consistently report lower levels of confidence than banks across several preparedness areas. Year-over-year results also show a modest decline in confidence across all tracked categories. This doesn't necessarily suggest institutions are less prepared, but possibly heightened awareness of emerging risks or increased organizational caution.

Expert Perspective

Our experts cautioned that high confidence does not always equate to true readiness, and that respondents in non-technical roles may be overestimating their institution's capabilities. Even with muted confidence year-over-year, respondents' self-assessments may still be overly optimistic. Cyber risk is complex, and real preparedness requires ongoing testing and honest assessment.

Cybersecurity education effectiveness may also be overestimated: while 86% of respondents say programs are effective or highly effective, our experts' observations suggest actual engagement in training sessions is often low, leaving room for improvement.

Finally, the data reveals an important tension: 87% of respondents report having a trusted cybersecurity partner, yet 27% aren't confident they wouldn't be found negligent after a breach. Knowing who to call and what steps to take in the first moments of an incident are essential to mitigating the damage and improving recovery. Immediate, actionable support is essential.

"Embracing AI and data analysis is key, but strong cybersecurity remains critical."

Source: Survey Participant

Return to main section

Focus on Cybersecurity Compliance

Cybersecurity compliance continues to grow in importance, requiring financial institutions to maintain a secure IT infrastructure, actively mitigate risks and follow complex regulatory rules.

Respondents identified several methods they prioritize as part of their cybersecurity compliance strategy, led by tools like multi-factor authentication and expanded training for senior leaders.

58%

Using Cybersecurity Tools like Multi-Factor Authentication (MFA)

▶ **Institution Variance:** Banks 62% | CUs 41%

55%

Increasing Cybersecurity and IT Training for Senior Management and Board

50%

Conducting Risk Assessments and Impact Analysis Studies

49%

Using Cybersecurity Frameworks (e.g., NIST CSF 800-53)

42%

Partnering with a Consultant for IT Governance Services

42%

Having Dedicated Architect, Data Officer and IT Operations Management Roles

38%

Establishing a Board-Level IT Governance Committee

36%

Defining Your Institution's Risk Tolerance

Industry Insight

Financial institutions maintain a high level of security relative to other critical industries, but even federal agencies like the CFPB—the nation's consumer financial watchdog—face cybersecurity compliance challenges.

An October 2025 audit by the Federal Reserve Office of Inspector General (OIG) concluded that the bureau currently lacks full awareness of its security vulnerabilities, showing that even well-resourced, federally funded government entities are struggling to keep up with evolving cyber threats and compliance.[19]

For community financial institutions, this underscores the importance of aligning controls, documentation and governance processes with continuously changing expectations.

Expert Perspective

Cyber compliance is not a checklist exercise. It requires ongoing evaluation of tools, processes and vendor capabilities. Institutions should regularly ask whether their controls function as intended, whether staff understand the risks those controls address and whether investment in additional safeguards are needed.

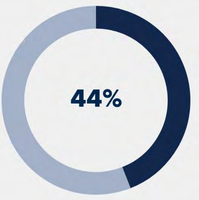
Though it can be challenging to implement effectively, MFA remains a top priority, and institutions that have implemented it over the past two years have made significant progress. Experts also highlighted that board-level IT governance committees are gaining traction, a positive indicator that institutions are stepping up compliance and oversight.

Return to main section

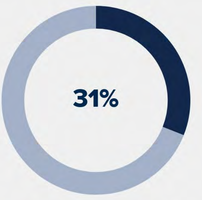
Budgeting for Cybersecurity

A growing share of IT budgets is allocated to cybersecurity, with three-quarters of respondents allocating 11–20% of IT funding. With cyber threats escalating in both frequency and severity, sufficient investment in prevention and mitigation is increasingly critical.

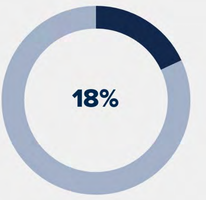
Cybersecurity Portion of Annual IT Budget



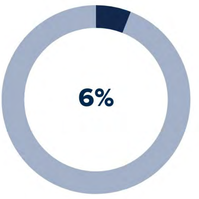
11% to 15% of IT budget



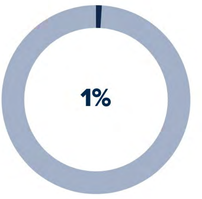
16% to 20% of IT budget



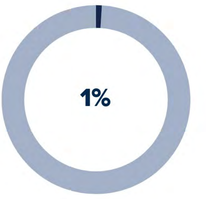
5% to 10% of IT budget



> 20% of IT budget



< 5% of IT budget



Don't Know

Industry Insight

Heading into 2025, Gartner forecasted that global information security spending would grow by 15%.[20] Given the rise of AI-enabled attacks, emerging digital asset technologies and expanded digital connectivity, this upward trend is likely to continue through 2026.

Expert Perspective

While some institutions are allocating 16–20% of their IT budgets to cybersecurity, our experts emphasized that higher spending does not necessarily indicate stronger protection. Measured, strategic investment is more important than targeting a specific number in budget planning.

Overspending in certain areas can even be counterproductive. Cyber liability insurance, for example, may not provide comprehensive protection, with as much as 75% of breach-related losses typically falling outside policy coverage. Our experts underscored that insurance should complement, not replace, a layered cybersecurity strategy built around prevention and mitigation.

High-impact controls don't necessarily require large budget increases. Cost-effective methods like high-quality security awareness training, regular testing and clear incident response planning are all essential elements of a robust program and can strengthen an institution's cybersecurity posture.

Investing in AI and cybersecurity isn't just a strategic move. It's essential to earning customer trust and staying competitive in a rapidly evolving financial landscape."

Source: Survey Participant

Return to main section