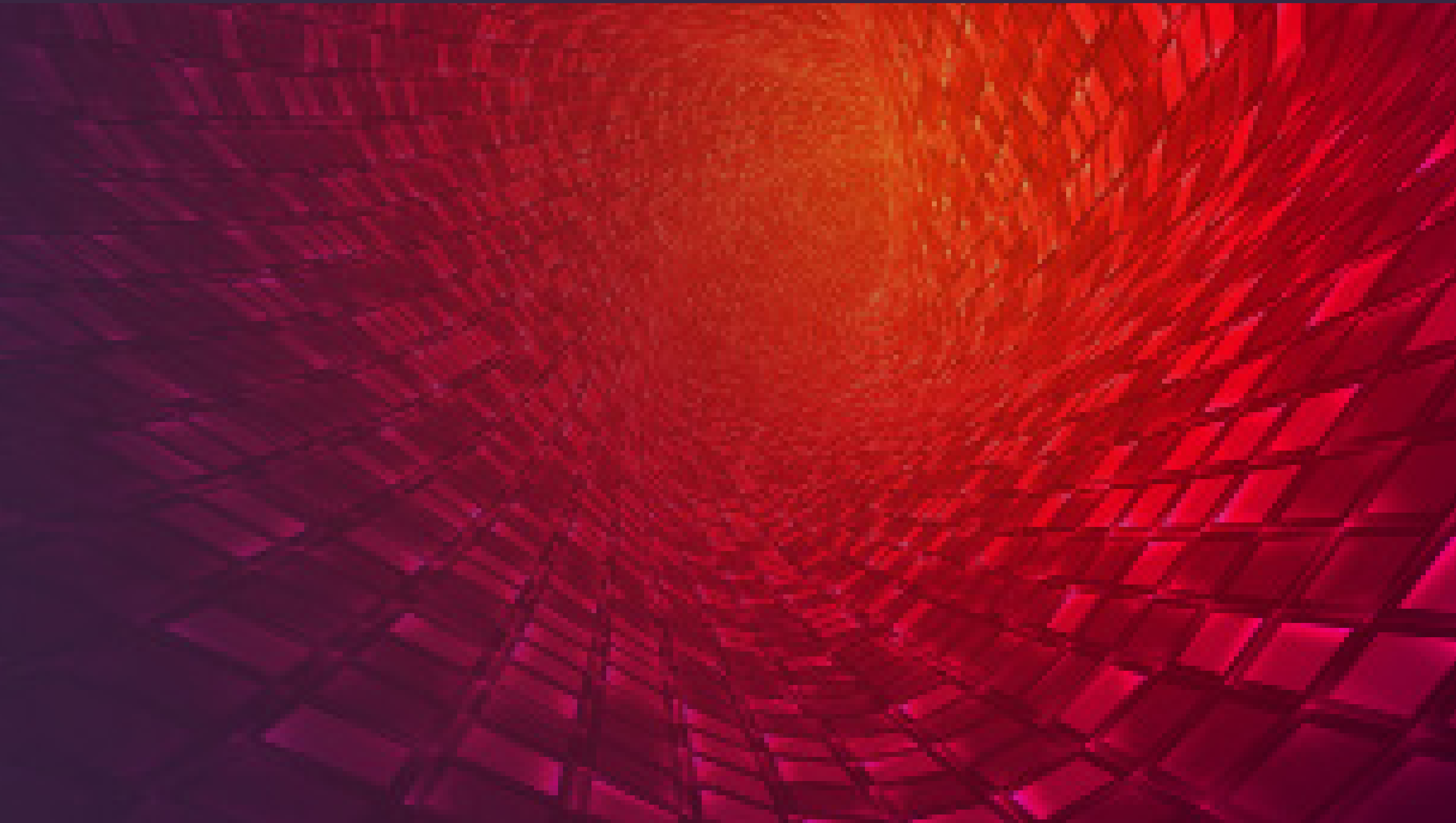
Integris

2026 Banking trust and technology report

Banks are spending more on technology without a clear picture of where the money goes—while fears surrounding cybersecurity and AI-driven decisions continue to rise.



About this survey

This survey from Integris offers a snapshot of how banks and their customers are approaching 2026. Customer trust in banks remains high–nearly 9 in 10 customers are confident that their bank keeps their information secure–but concern is rising over cybersecurity threats and the expanding use of AI in financial decisions.

Most customers say their bank is protecting their data, yet many report growing unease about potential security lapses or AI-driven mistakes. Forty percent listed “hackers stealing bank data” as their greatest concern–more than phishing, insider errors, or mobile-app fraud combined. More than half (52%) worry that AI systems could mistakenly freeze their account access, reflecting a new layer of anxiety surrounding automated decisions.

Banking executives report similar pressures. Nearly half (45%) expect technology budgets to rise 40% or more in 2026, and 18% anticipate increases above 60%. At the same time, 64% say they do not have full visibility into total IT spending across their institution, as costs are spread over departments, vendors, and legacy systems. Banks also report reliance on managed service providers (MSPs) for critical capabilities, with 70% of surveyed institutions depending on managed service providers for key IT functions, such as advanced cybersecurity support. This heavy reliance on MSPs makes external partnerships central to daily operations and security.

Combined, the findings show banks moving to strengthen security and update aging infrastructure as customer expectations shift. How well institutions manage cybersecurity risks, AI governance, and communications will determine whether current levels of confidence hold in the year ahead–and beyond.

Cal Roberson
Vice President, Financial Institution Division
Integris

The purpose of this report

This report draws on two national surveys conducted in November 2025: a Pollfish survey of 1,000 U.S. banking customers, and a Censuswide survey of 673 U.S. banking executives from small and midsize institutions ($20 billion in assets or less) that outsource all or part of IT to an MSP. Bank respondents included chief information officers, chief technology officers, chief information security officers, chief financial officers, compliance officers and IT directors. The combined data offers insight into the following:

- Customer expectations around cybersecurity, fraud protection, communication, and artificial intelligence (AI) use in banking
- Executive preparedness to meet those expectations in practice
- Gaps between customer confidence and institutional capabilities
- Modernization pressures that weigh more heavily on community banks

Together, these perspectives outline the operational and security issues likely to shape banking in 2026.

Key findings

Top takeaways from the dual surveys of banking executives and customers include the following:

Findings for bank executives:

- **64%** lack visibility into total IT spending because costs are scattered among departments, vendors, and legacy systems.
- **51%** reported a significant email-based breach in the past year; **50%** reported a mobile-related breach.
- **45%** expect technology budgets to expand by 40% or more in 2026; **18%** anticipate budget increases of more than 60%.
- Cybersecurity, compliance automation, AI governance, and data integration top the list of modernization priorities for 2026.

Findings for bank customers:

- **51%** chose their bank primarily because they trust its security.
- **40%** name malicious attackers stealing bank data as their biggest concern in banking.
- **67%** would consider switching institutions after a serious breach at their bank.
- **52%** fear that AI could wrongly freeze their account or block transactions.
- **15%** say their bank rarely or never communicates about security updates.

Analysis and insights

Banks are spending more on technology–despite uncertainty about where that money goes

Bank executives say digital modernization is overdue–and they are supporting it with major budget increases. About 45% of executives expect their technology budgets to jump by 40% or more in 2026, while 18% expect budget increases of more than 60%. These investments reflect rising security pressures, cloud expansion, surging digital channel usage, and new AI tools. However, modernization is complicated by legacy systems, fragmented departments, and heavily regulated environments. Many institutions operate on technology architecture built up over decades, with layered integrations that cannot be easily replaced or unified. This complexity creates real barriers: Executives must modernize critical systems without disrupting the "always on" services that customers expect. In effect, banks are trying to refurbish the airplane while still flying it–a modernization paradox. The risk is that malicious attackers and nimble competitors may move faster than community banking institutions can re-architect their core systems.

Critically, banks are pouring money into technology without always knowing where it goes. Despite rising budgets, 64% of executives admit they are "not sure" how much their bank spends on IT in total. This lack of visibility into IT spending impedes prioritization, weakens vendor oversight, and complicates efforts to measure ROI on new initiatives.

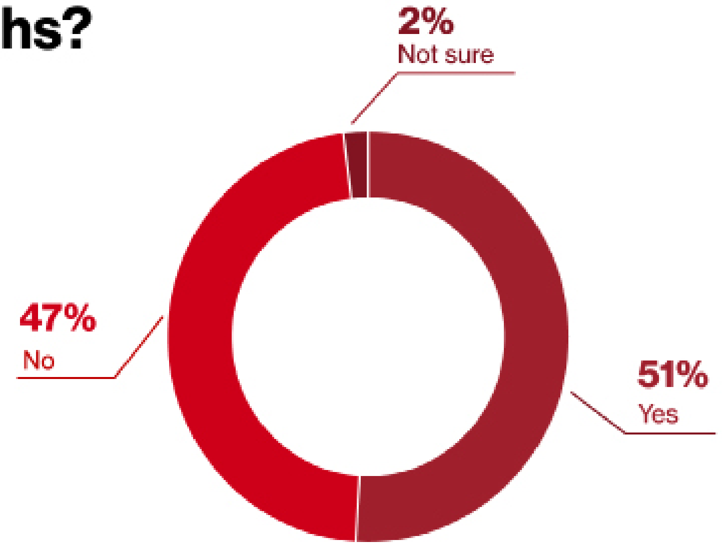
In other words, modernization requires not just more investment but better IT investment governance. Distributed technology spending, inconsistent data governance, and siloed decision making all slow progress even as technology spending increases. Breach data underlines the urgency to spend wisely with more than half of banks experiencing email and mobile breaches in the last year. Institutions are not modernizing for hypothetical threats–they are responding to active incidents. Without clearer tracking of IT expenditures and outcomes, banks risk inefficient spending that fails to adequately reduce those very threats.

In 2026, community banks will face pressure to apply their technology spending wisely to create secure customer experiences, protect data on the back end, and ensure system uptime and security.

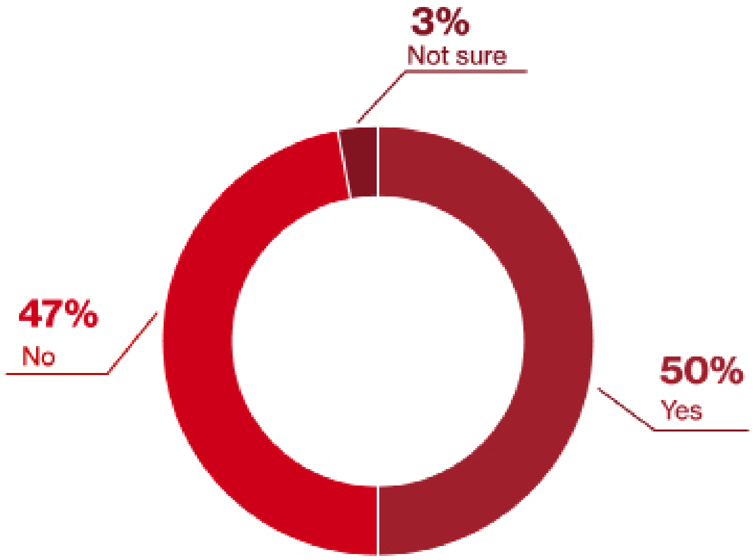
Banks are experiencing far more security incidents than customers know

Banks are facing far more security incidents than the public realizes. According to the executive survey, 51% of institutions suffered an email-based breach in the past 12 months, and 50% experienced a mobile-device breach in that time. These figures illustrate that breaches are now a routine operational risk throughout the industry–not isolated attacks.

Has your organization experienced any significant email-based security breach incidents in the past 12 months?



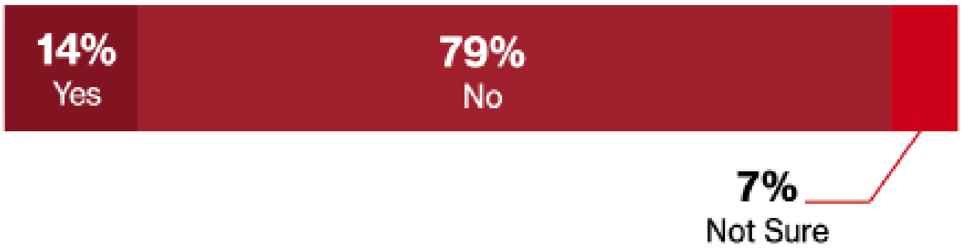
Has your organization experienced any security breaches involving mobile devices in the past 12 months?



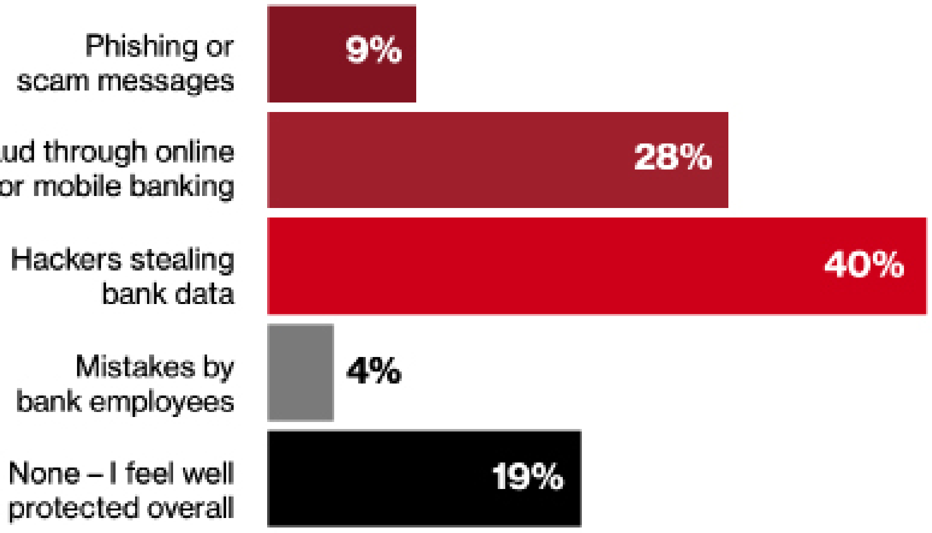
Customers are largely unaware of how common bank breaches are. Only about 1 in 10 customers report receiving a breach notification from their bank in the past year, and a majority (57%) believe their bank has never been breached. This lack of awareness shapes consumer expectations, because most customers have never experienced a bank breach, they assume their own institution has largely avoided attacks. That assumption sits alongside deep anxiety about cyberthreats. In the customer survey, 40% list “malicious attackers stealing bank data” as their biggest fear–about as much as phishing, insider errors, or mobile app fraud combined.

Regardless of their bank’s size or cybersecurity budget, customers increasingly expect their bank to operate with the defenses of a national institution: instant threat detection, rapid alerts, and zero errors that could jeopardize account access.

Have you ever, at any time, been notified by your bank that your data or account was involved in a security breach?

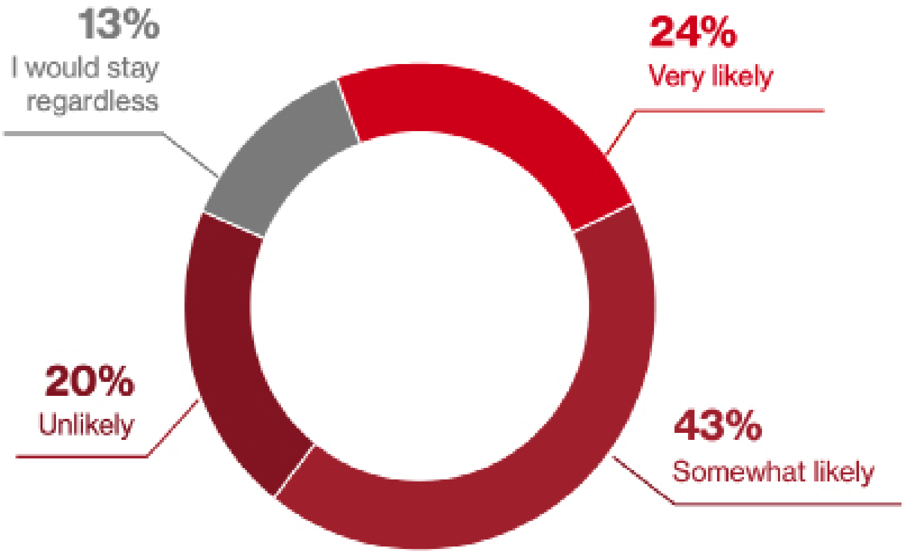


What cybersecurity threat concerns you the most when it comes to your bank?



Yet, in spite of the frequency of breaches, customers rarely hear about these vulnerabilities from their bank. When communication is limited, even minor incidents can damage confidence. This “breach-perception gap” creates a fragile trust dynamic: Customers trust their bank until the moment that trust is broken. Indeed, 67% of customers say they would likely switch banks after a serious breach, with nearly a quarter “very likely” to do so. As customers also grow more uneasy about AI-driven decisions and automated account controls, the stakes for maintaining trust through security measures only increase.

If your bank experienced a serious breach in the future, how likely would you be to switch to a different bank?



Trust in banks is high, but based on familiarity

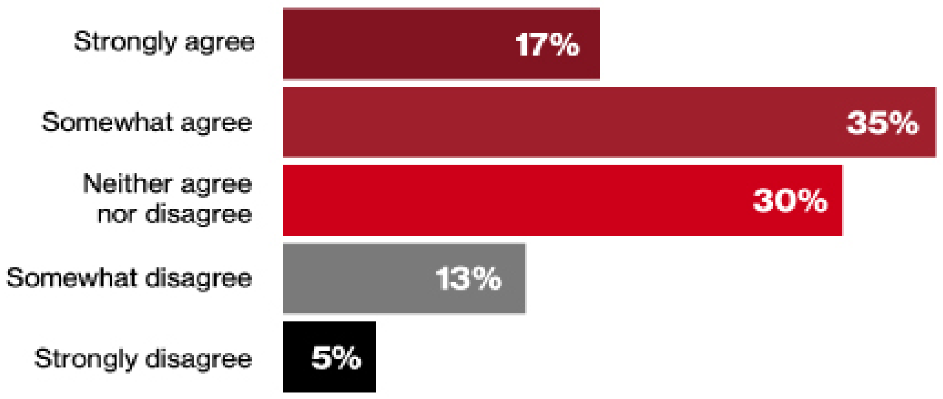
Nearly 9 in 10 customers say they trust their bank to protect their personal and financial data, which is an extremely high confidence level (88% express security confidence). But much of that trust appears to be based on familiarity rather than on any true understanding of *how* banks defend against threats.

Many customers simply assume that their bank is secure because they've never seen evidence to the contrary. In fact, 88% of customers reported no breach notifications from their bank in the past year, reinforcing a sense that "breaches don't happen here." At the same time, a significant share of customers lack knowledge about the policies and technologies their bank has in place. For example, 23% say they do not understand how their bank uses AI in its services.

This dynamic makes customer trust vulnerable. Because consumers believe their banks are safe *until proven otherwise*, a single public breach or high-profile failure can swiftly upend years of assumed security. With two-thirds of customers saying they'd switch institutions after a breach, customer loyalty has become increasingly fragile. Because trust is anchored more in *perceived* security than in transparent knowledge of safeguards, it can be a false foundation. Trust in banks often rests on an assumption rather than fact–and assumptions can collapse quickly in a crisis.

AI is emerging as a major trust flashpoint

As AI becomes more integrated into fraud detection, risk scoring, customer service, and transaction monitoring, customers are voicing heightened concern about how these automated decisions might affect them. Some 52% of customers worry that AI could mistakenly freeze their accounts or block legitimate transactions, and about 40% fear that AI usage by their bank might expose personal data. These concerns sit alongside significant uncertainty: nearly one-quarter of customers (23%) say they don't understand how their bank uses AI at all. To many consumers, AI systems are black boxes that lack transparency. The prospect that AI could make mistakes seems as alarming as a traditional security breach. In consumers' eyes, if an algorithm creates an erroneous fraud flag or account freeze, it is tantamount to a security failure. It prevents customers from accessing their money, undermining trust.



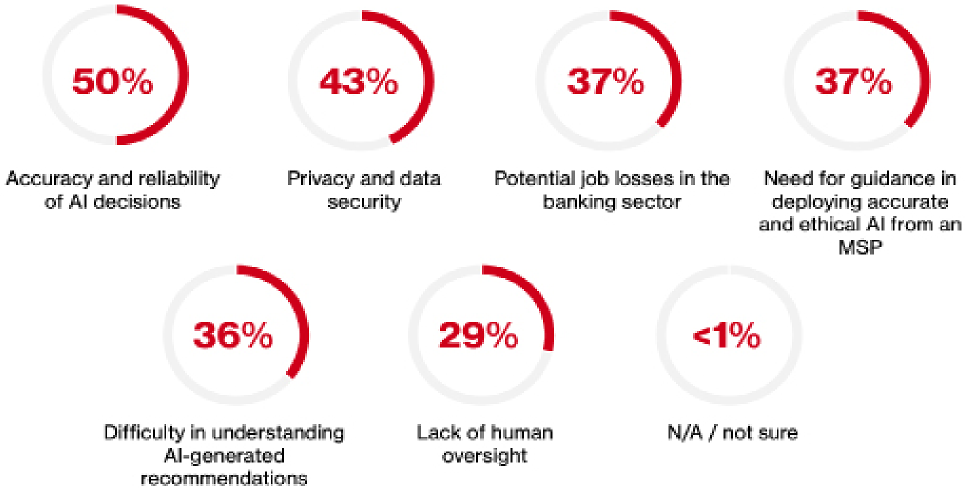
How much do you agree with this statement: "I worry that AI systems could lock me out of my banking accounts by mistake."

The rapid adoption of AI within financial institutions amplifies uncertainty. While executives cite AI as a boon for efficiency and threat detection, more than a third of banking leaders report challenges interpreting AI outputs or understanding how certain AI-driven decisions are made. If banks can't clearly articulate how AI decisions are being used and overseen, customers may lose trust in the institution. AI governance and reliability, therefore, must be treated as part of a bank's trust infrastructure, not as optional technical projects. In practice, that means banks need to put guardrails around AI–from rigorous testing and human-in-the-loop oversight to transparent customer communication about how AI is used in their accounts.

AI adoption inside banks surges–but oversight hasn’t caught up

While AI adoption is widespread, governance is lagging. More than 36% of executives say they struggle to interpret the outputs of AI systems or to understand how certain algorithmic recommendations are generated. This disconnect raises two urgent concerns: internal risk and external perception.

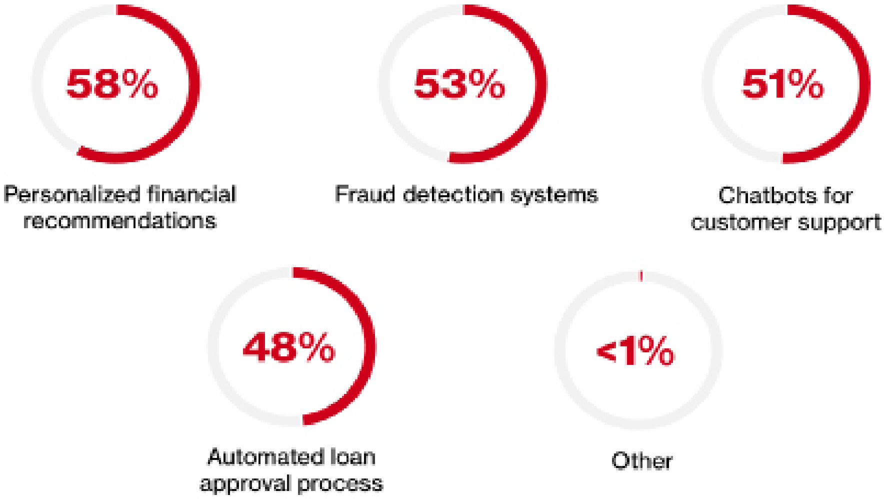
What are your top concerns about the use of AI in banking, if any? (Select up to three)



Internally, if teams cannot fully explain how AI arrives at decisions, they cannot reliably audit results, ensure fairness, or maintain regulatory compliance. Externally, customers’ uncertainty about AI (and occasional high-profile AI errors) intensifies worries about automated account actions. This uncertainty varies sharply by institution type: 41% of community-bank customers and 27% of large-bank customers say they are “not sure” how their bank uses AI in services or decision making. That gap points to a transparency and education disadvantage for smaller institutions, which often have fewer resources to explain new technologies to their customer base.

As AI becomes embedded in more critical functions, banks must shift from mere adoption to robust oversight. This means documenting AI models and decisions, instituting human-in-the-loop review for high-stakes outcomes, formalizing escalation paths for AI-driven issues, developing AI acceptable-use policies, and strengthening transparency protocols both internally and with customers. AI that is fast but opaque may accelerate operations, but it erodes trust. AI that is explainable, well-supervised, and clearly communicated can become a trusted asset rather than a liability.

What AI-enabled banking services have you deployed, or do you plan to use in the next 12 months? (Select all that apply)



Communication gaps make customers feel less safe–even when protections exist

Trust in banking security isn't based only on outcomes; it's also reinforced (or undermined) by communication. And there is a communication disconnect: 15% of customers say their bank "rarely or never" communicates with them about security measures or updates, and nearly half say such updates are infrequent at best. Without regular communication, customers may underestimate the protections their bank already has in place or fail to notice improvements. This perception gap can quietly erode trust even when a bank's actual cybersecurity controls are strong.

Customers increasingly expect banks to communicate the way consumer technology companies do–with proactive notices, clear explanations of new features or threats, and transparency about a bank's measures to keep accounts safe. Bank silence becomes a signal of vulnerability. If a bank isn't talking about security, some customers assume it isn't doing enough to secure data.

On the executive side, limited visibility into IT operations (as noted, 64% of leaders lack a clear view of total IT spending) and complex webs of vendors make effective communication even more challenging. Bank leaders may not have a simple answer to give to the public about "how we're protecting customers," because internally that information is spread across multiple teams and partners.

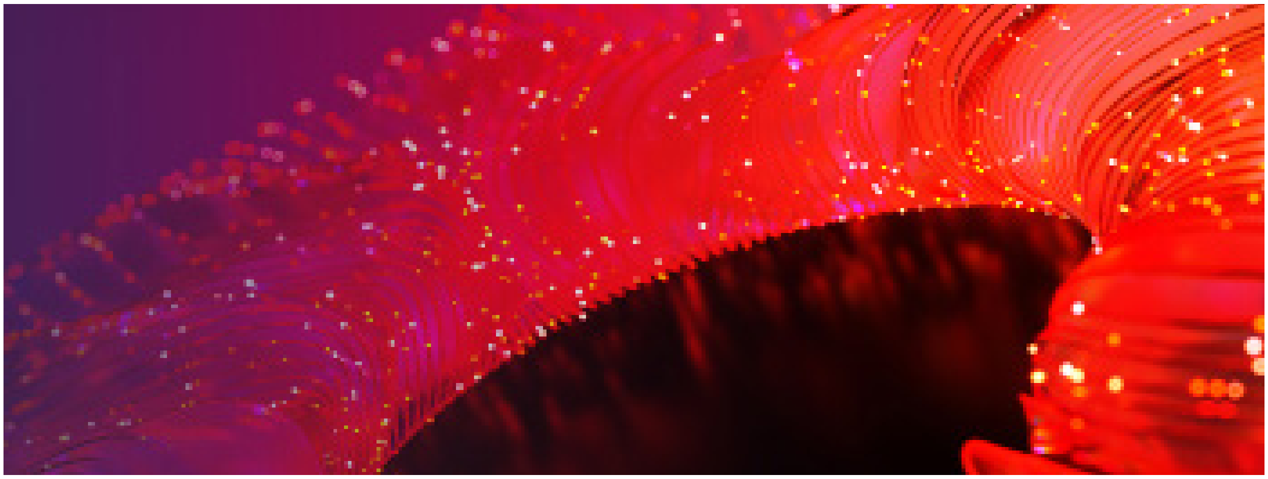
The result is an information vacuum where customers fill in the blanks with worst-case assumptions. Going forward, establishing a consistent security communication cadence with customers is becoming as important as improving the technical controls themselves.

In 2026, banks will need to not only be secure but also convince customers of that security through frequent, transparent updates.

Community banks: A distinct modernization challenge

Community-bank customers expect the same level of cybersecurity, fraud protection, and digital reliability as customers of the nation's largest banks–but smaller institutions face unique headwinds in meeting customer expectations. The data shows that community-bank customers often have a *stronger baseline of trust* in their local institutions' safety, likely because of more personal relationships and a lack of negative incidents.

For instance, community bank customers have experienced fewer security incidents: **a majority (66%) believe their bank has never been breached, notably higher than the 53% of large-bank customers who believe the same.**



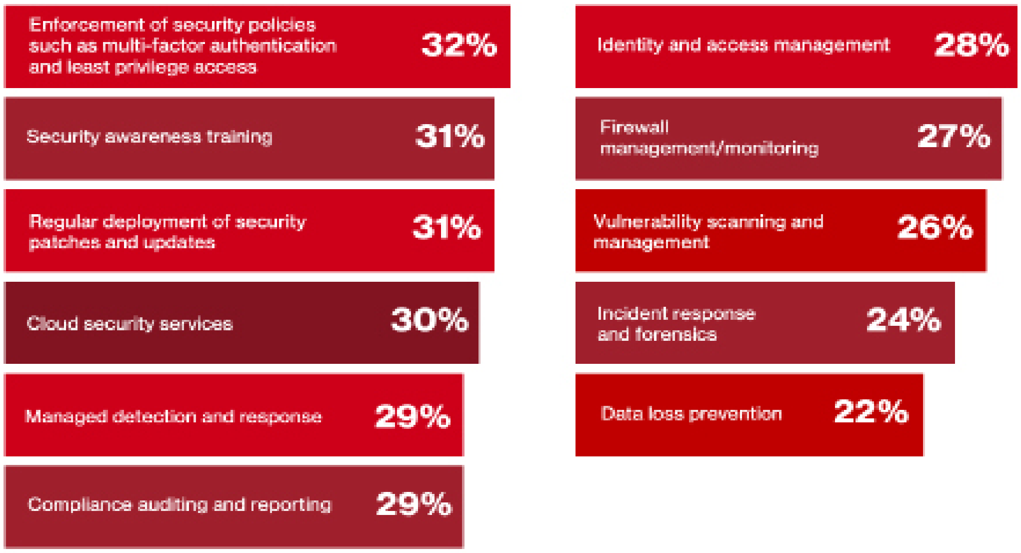
Community banks' trust advantage can evaporate quickly if consumers' assumption about bank security is shattered by a serious accident. In fact, while about 72% of large-bank customers say they were "very" or "somewhat" likely to switch banks after a serious breach, a still-substantial 57% of community-bank customers say they would consider leaving their bank under the same circumstances. More loyalty remains at community banks, but not enough to shield them from reputational damage if a breach occurs.

Another challenge is the transparency gap surrounding new technologies such as AI. As noted, 41% of community-bank customers are not sure how their bank uses AI (versus 27% at large banks), suggesting that smaller institutions are struggling to communicate their modernization efforts. The pattern is consistent: Community banks often enjoy stronger personal connections with customers, but they may be perceived as having weaker technological capabilities or less openness about those capabilities. With customers now benchmarking all institutions against the digital performance of big banks and fintechs, smaller banks face sharper pressure to modernize. Closing the gaps in AI transparency, security communication, and core IT resilience will determine whether community banks can maintain their long-held trust advantage in the coming years. Investments in modern infrastructure, combined with proactive customer education, will be critical so that community institutions can meet big-bank standards without losing the personal touch that differentiates them.

MSPs are central to bank operations–but key gaps remain

The results show just how integral managed service providers have become to banking IT. Survey data indicates that banks outsource the majority of their core IT functions to MSPs, with well more than 80% of institutions relying on external providers for cybersecurity, cloud operations, data backup and disaster recovery, help desk support, and IT strategy guidance. In particular, 87% of surveyed banks say they use an MSP for basic cybersecurity, 87% for advanced cybersecurity, 87% for backup/DR, and 85% for cloud services. In effect, MSP partnerships now run much of the technical backbone of banking operations. This concentration makes MSP capabilities–and their potential shortcomings–central to a bank's security and modernization outcomes.

What cybersecurity services does your MSP provide, if any? (Select all that apply)



However, outsourcing hasn't fully solved pain points. Interestingly, the same areas where MSPs are most involved remain the most challenging for banks. Executives identified persistent issues such as data-integration challenges (cited by 49% of respondents), IT planning and architecture gaps (42%), ongoing security concerns even with MSP support (37%), AI implementation difficulties (32%), and compliance and audit strains (31%). In many cases, banks lean on MSPs for help with these issues–for example, automating compliance reporting or deploying new AI-driven security tools–yet the survey suggests these remain top burdens.

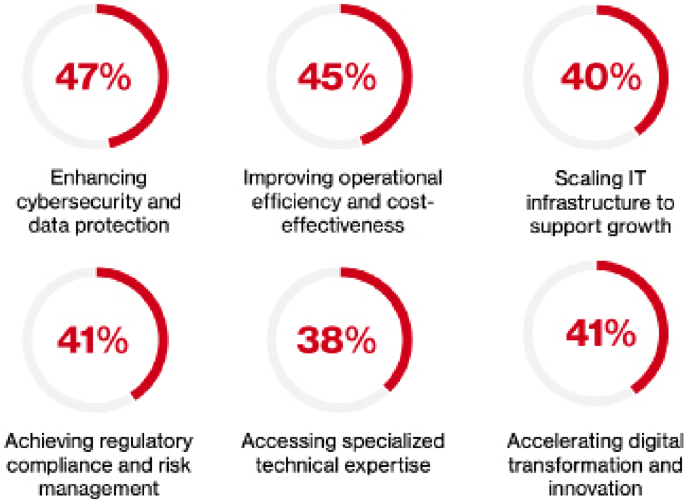
Even in regulatory audits, where banks often use MSP-provided automation and documentation, compliance management continues to be resource-intensive.

Looking ahead, banks plan to increase use of MSPs in various areas in the next 6-12 months: advanced cybersecurity (42%), cloud services (41%), IT consulting and strategy (38%), compliance and regulatory support (34%), and AI implementation and management (32%). This means expectations on MSPs will rise even further in 2026.

For MSP providers, the mandate is clear: Simply taking over IT tasks is not enough. Banks now need deeper visibility into MSP-run environments, tighter integration between outsourced services and in-house systems, and stronger governance–especially surrounding sensitive domains such as security and AI.

In short, outsourcing must be coupled with oversight. Traditional MSP models will have to evolve to help banks close operational gaps and meet higher standards for transparency and risk management.

What are the primary objectives your institution aims to achieve through its partnership with an MSP, if any? (Select up to three)



Conclusion: Continuing to build consumer trust

The dual surveys paint a picture of a banking sector caught between accelerating threats and increasing consumer expectations. Customers trust their banks, but that trust can falter quickly after a visible breach or a high-profile AI error. Executives understand the need to modernize and are preparing for major increases in technology spending to do so. But structural complexity, fragmented systems, and legacy infrastructure continue to slow down progress. Community banks, in particular, face the challenge of meeting big-bank expectations with smaller budgets and greater MSP dependence, putting a premium on smart governance and clear communication.

> *"What we're seeing is that security and transparency are no longer separate conversations for banks,"* said Cal Roberson, vice president, Financial Institution Division at Integris. *"Customers expect clear communication around cybersecurity and AI, particularly after high-profile incidents, and banks are under pressure to meet those expectations while managing complex, legacy environments."*

Cal Roberson
Vice President, Financial Institution Division
at Integris

Cal has over 25 years of experience supporting technology for community banks and credit unions, most of it with Integris (formerly Caltech). As Vice President of the Financial Institution Division, he oversees strategic initiatives and partnerships while serving as a trusted partner to financial institutions, helping them navigate technology challenges and succeed in a rapidly evolving industry.

Integris.

Integris is a national leader in future-ready managed services in Cranbury, New Jersey, delivering innovative solutions that drive digital maturity for small to midsize businesses. We specialize in key industries like community banking, legal, manufacturing, nonprofit, healthcare, and more. We go beyond traditional IT management by delivering strategic roadmaps that optimize operations, strengthen cybersecurity, refine cloud solutions, and ensure compliance – all while enhancing our client's digital capabilities. Our goal is to transform each organizaion into a smarter and faster digital powerhouse. Our platform is responsive, secure, and ready to meet the unique regulatory demands of the industries we serve. With Integris, you get enterprise-level IT with a personal, industry-focused touch. To explore our product offerings, visit our website at integrisit.com.