JONES WALKER

2024

Community and Mid-Size Banks
Cybersecurity Survey

joneswalker.com

Inside the Survey

Executive Summary 05

Foreword 06

Top Takeaways 08

Survey Methodology 10

Takeaway 1
Post-Incident Regulatory Compliance is Slowly Improving, but Prevention and Preparedness are Lacking 16

Takeaway 2
The Lack of Due Diligence Performed on Third-Party Vendors is a Significant Risk 28

Takeaway 3
Banks Are Underutilizing Outside Counsel and Cybersecurity Expertise 40

Takeaway 4
Responsibly Embracing Emerging Technology Delivers Significant Advantages 46

Conclusion 52

Additional Resources 54

99%

of community and mid-size banks report that the industry is very or somewhat prepared for a cyberattack.

However, most banks (62%) feel that there is room for improvement.

99%

of the respondents' banks rely on third-party vendors to support all or at least part of their cybersecurity programs.

However, consistent due diligence and oversight appear to be lacking.

90%

of respondents' banks prioritize compliance by focusing on breach notification and other regulatory requirements.

However, a significant number of the banks surveyed report that they are failing to implement or enforce standard protocols such as data encryption.

> Cybersecurity is one of the most significant risks facing the banking industry in today's electronic environment. Banks are focused on preventing and managing this risk, but cyber threats continue to evolve. The **2024 Jones Walker Cybersecurity Survey** is a meaningful resource showing ways the surveyed banks are currently managing cybersecurity risk. Bankers can compare their practices with the survey results to identify possible changes or to confirm that they are in-step with the industry.
>
> **David Boneno,** General Counsel, *Louisiana Bankers Association*

Executive Summary

Welcome to Jones Walker LLP's **2024 Community and Mid-Size Banks Cybersecurity Survey** report, the fourth in our biannual series of industry-focused cybersecurity studies. Like our prior three surveys, which also examined the importance of cybersecurity in critical infrastructure-related industries (maritime, energy, and ports and terminals),[1] this year's report considers the current state of cybersecurity in community and mid-size banks, one of the most important segments of the financial services industry.

Cybersecurity events continue to impact businesses on a daily basis, and banks are no exception. Indeed, financial services organizations, and banks in particular, are among the most attractive targets of cybercriminals.[2] Regardless of the cause, cybersecurity events are disruptive, damaging to customer trust, and expensive. Just last year, financial institutions contended with the highly publicized MOVEit data breach that affected tens of millions of businesses[3] and the National Public Data breach that may have exposed the personal information of nearly 3 billion individuals.[4] Earlier this year saw spikes in phishing and other malicious activity that followed the widespread outages caused by the flawed CrowdStrike cybersecurity update.[5] Together, this activity confirms that cyberattacks continue to rise in frequency, sophistication, and cost.

In April 2024, the International Monetary Fund (IMF) reported that the financial sector has suffered more than 20,000 successful cyberattacks over the past two decades, nearly half of which were committed against banks. The IMF also estimated the maximum potential direct cost of a single cyber event has more than quadrupled since 2017, to $2.5 billion, and estimated the indirect losses (such as reputational damage or security improvements), while difficult to quantify, could be even higher.[6]

Our 2024 Community and Mid-Size Banks Cybersecurity Survey report is designed to assess the state of cybersecurity awareness, confidence, and preparedness in the critical business of everyday banking within our communities and regions. After gathering and analyzing responses from 125 bank executives, including senior risk, technology, and information security leaders, we identified four important takeaways:

- Banks should enhance their focus on prevention and preparedness.
- Banks would benefit from increased oversight of third-party vendor relationships, as these are a significant source of exposure.
- Outside experts and legal counsel are underutilized, risking increased exposure.
- Banks should embrace innovation (including emerging technologies) as a differentiator and to improve diligence, preparedness, and oversight.

We hope that this report will provide useful information as you continue to secure and strengthen your organization against cyber threats. We also invite you to contact us for more information on how Jones Walker can support your cybersecurity compliance and governance programs, technology and artificial intelligence (AI) procurement, deployment and use, third-party vendor contracting and diligence, and breach preparedness and response.

Foreword

Community and mid-size banks, or those with less than $50 billion in assets, account for the vast majority of banks in the United States. These banks hold approximately 36% ($4.5 trillion) of all outstanding loans and more than $6.7 trillion in assets. Importantly, these banks also employ a workforce of nearly 755,000 people.[7]

In today's fast-paced digital landscape, virtually every business has become a technology-driven enterprise, including those in the banking sector. As much as any organization, banks are subject to the business imperatives of digital transformation, and most are increasingly dependent on third-party cybersecurity and technology solutions to modernize and remain competitive.

Unfortunately, digital transformation comes with significant financial, operational, and reputational risks. According to the 2024 IBM/Ponemon *Cost of a Data Breach Report*, the global average cost of a data breach has increased 10% over the prior year, to $4.88 million.[8] The United States has the highest average data breach cost, at an average cost of $9.36 million per breach event ($6.08 million per event in the financial industry) — a breathtaking number that would cripple most businesses.

In addition to the volume of data impacted, the cost of a data breach is typically commensurate with the sensitivity of the data involved. Accordingly, losses from the disclosure of sensitive personal information and financial data could be even higher. In addition to these direct costs, banks that sustain a cyberattack stand to suffer significant brand damage and diminished customer confidence in the wake of such an incident. Just as community banking is largely a reputation business, cyber risks have the potential to significantly impact reputation.

> A shortage of skilled cybersecurity professionals is a key contributing factor to this increased breach threat.

According to the recently released *2024 Security Budget Benchmark Summary Report*[9] of chief information security officers (CISOs), published by IANS Research and Artico Search, cybersecurity staff growth has slowed significantly, declining from 31% in 2022 to 12% in 2024.

However, while cybersecurity staff has declined, the IANS/Artico report found that CISO-allocated budgets had grown 8% from 2023 to 2024. Although this figure is below the 2021 and 2022 growth rates (16% and 17%, respectively), this continued growth in security-related spending underscores the benefits of investing in technology solutions to bolster information security programs — including emerging technologies such as AI.

Early involvement of regulatory and law enforcement authorities also appears to mitigate the impact of a breach. For example, in its *2024 Data Breach Investigations Report*,[10] Verizon found that when investigators from the Internet Crime Complaint Center of the FBI went to work on business email compromise cases, they were able to recoup 79% or more of losses in at least half the matters.

Other positive factors include the increased focus of organizations on cybersecurity as a board-level issue and a broad recognition of the importance of acting quickly to mitigate negative impacts. Many are predicting that implementation of emerging technologies such as AI in the cybersecurity space will further assist organizations in rapidly identifying the presence of vulnerabilities in their systems and data loss.[11] Use of emerging technologies such as AI for cybersecurity must also be evaluated carefully, however, as there are "challenges and opportunities to enhancing the safety and security of system applications from cyberattacks" using AI tools generally.[12]

Despite evident progress, it is clear that cybercrime remains lucrative and is attracting more and more criminals to the game. Threat actors are becoming more creative, elusive, and sophisticated and are learning better ways — including their own use of AI[13]— to evade the increasingly refined defenses of businesses and other organizations.

This 2024 survey is designed to assess the current-state preparedness of community and mid-size banks to prevent, identify, and respond to cyberattacks and to explore specific actions such banks can take today to increase their cyber resilience and preparedness. One of our primary findings is that, unfortunately, community and mid-size banks have additional work to do to strengthen their cyber preparedness in accordance with regulatory and industry standards. While government agencies, trade and industry associations, and public-private initiatives can serve as a good source of guidance and resources as to industry standards, the ultimate responsibility to maintain regulatory compliance and to secure and protect sensitive data in their control falls squarely on the shoulders of community and mid-size banks themselves.

Whether you are a stakeholder in the financial services industry, an executive or employee of a community or mid-size bank, or a business or individual who utilizes financial services in your daily life, we hope you will find the information set out in this survey useful. We encourage you to use this survey as a tool in assessing — and enhancing — your awareness of the importance of cybersecurity in the banking space and bolstering your organization's cyber readiness.

Top Takeaways

01

+ Post-Incident Regulatory Compliance is Slowly Improving, but Prevention and Preparedness are Lacking

Given the highly sensitive data in the care, custody, and control of banks and the highly regulated nature of the banking industry, it makes sense that compliance with federal and state regulations governing data security and privacy is a top priority for banks and an area of continued focus for regulators. While the majority of our survey respondents indicated that they feel that the banking industry is very (38%) or somewhat (61%) prepared for cyberattacks, there appears to be a tendency to focus more on *post-incident* regulatory compliance (including understanding breach reporting and notification-related obligations) than to proactively invest in pre-incident preparedness and prevention activities.

In a nutshell, **community and mid-size banks are likely not focusing enough attention on preparedness and prevention activities that will prevent data breaches and assist in a rapid and organized response if and when a data breach or other cyber event occurs.** Such activities include employee training, developing and maintaining an incident response plan (IRP), and testing the IRP's effectiveness (such as through regular tabletop exercises), regular penetration testing, establishing and enforcing data encryption standards, implementing AI solutions, and imposing similar obligations on their critical third-party vendors.

02

+ The Lack of Due Diligence Performed on Third-party Vendors is a Significant Risk

In recent years, the focus of regulators has expanded to include the level of scrutiny that banks are imposing on their third-party vendors and such banks' own internal security controls. This is in large part due to the growing reliance of banks — particularly community and mid-size banks — on third-party vendors to support their information security controls.

A staggering 99% of our survey respondents reported using third-party vendors to perform cybersecurity-related functions. A full 90% reported leveraging third-party vendors to support critical open banking, banking-as-a-service, and other financial technology (fintech) platforms.

Leveraging external vendors provides community and mid-size banks with significant opportunities to scale using their existing resources, obtain niche expertise that may not otherwise be available in their locality, and continue to modernize their service offerings in order to retain and expand their customer bases. That said, it must not be forgotten that the ultimate responsibility for regulatory compliance remains with the banks themselves. Most banks perform pre-engagement diligence and maintain vendor oversight designed to ensure that their vendors provide compliant, effective services; however, careful attention is required to ensure that use of outside vendors does not inadvertently create unanticipated vulnerabilities.

03

+ Banks Are Underutilizing Outside Counsel and Cybersecurity Expertise

Community and mid-size banks are in a unique position to understand their local economies and the needs of their customers. **For a number of reasons (resource availability, costs, etc.), they cannot be expected to maintain an expert level of insight into rapidly developing, complex cybersecurity regulations, emerging technologies, and related best practices.** Engaging outside legal counsel and experts who are deeply familiar with these issues can help banks develop a comprehensive program that ultimately may be less costly than trying to implement solutions internally on a piecemeal basis.

Experienced legal counsel can also advise banks with respect to how the various players — insurers, consultants, government agencies, and public-private consortia — fit together in implementing a robust breach preparedness and response strategy. Involvement of outside counsel can be useful in ensuring that confidentiality and potentially privileged information are protected when engaging in discussions related to breach preparedness and response.

Experienced counsel can further serve as a resource for identifying, developing, and implementing strategies that can help banks better protect themselves and their customers. Such strategies range from implementation of emerging technologies to advising on robust terms and conditions in critical vendor contracts that can mitigate risk.

04

+ Responsibly Embracing Emerging Technology Delivers Significant Advantages

Technology can serve as a force multiplier for resource-intensive tasks, and cybersecurity is no exception. Organizations of all sizes and in all industries are realizing enormous efficiencies from the implementation of emerging technologies, including AI-enabled solutions. These technology solutions are no longer restricted to use in customer-facing services and internal operational tasks — they are also being used to optimize and transform dated security systems and processes.

Banks, like other organizations, should certainly exercise enhanced caution when exploring these technology solutions, particularly those that involve credit, lending, hiring, or other decision-making activities. In so doing, they can avoid inadvertently creating or acting on biases that run afoul of regulations or customer expectations.

There are, however, other applications for such technologies that can and should serve as an advantage, particularly to resource-constrained community and mid-size banks. **Emerging cybersecurity technologies can provide significant support in helping these entities strengthen their breach prevention, detection, and other preparedness capabilities.** Outside attorneys and technology experts can help identify and implement cost-effective, reliable cybersecurity solutions.

Survey Methodology

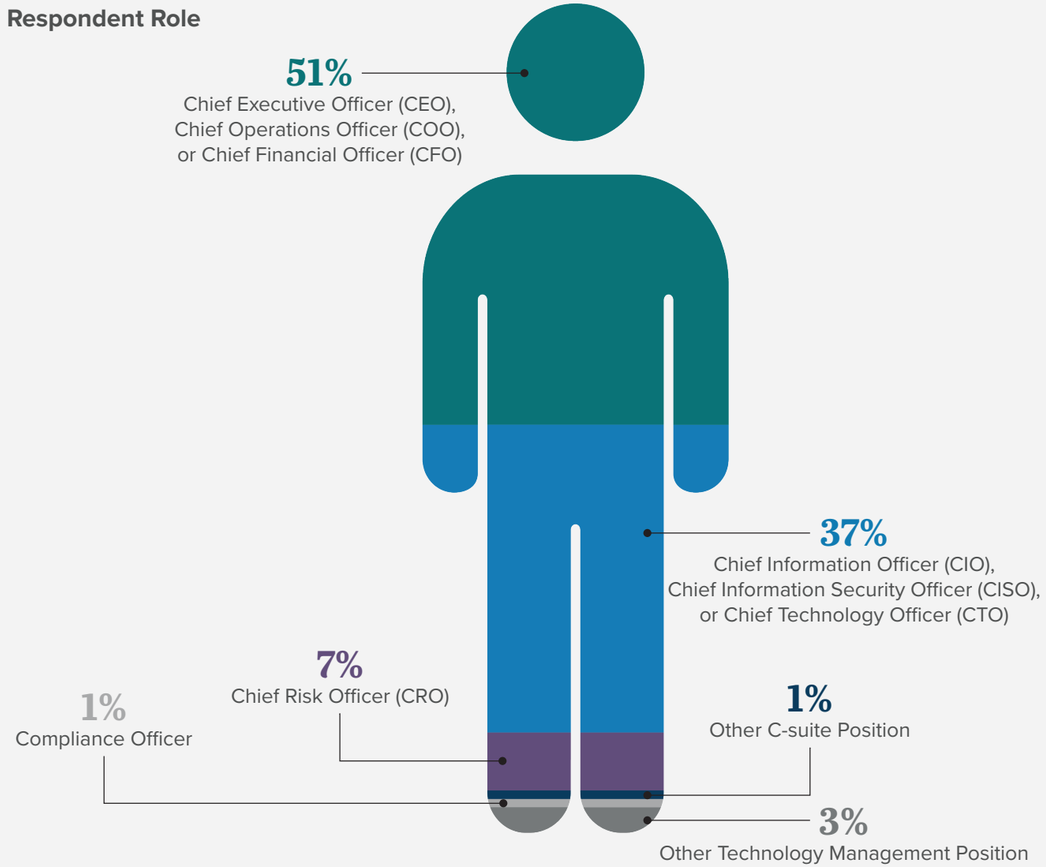
Sector: Community and mid-size banks in the United States with less than $50 billion in assets
Survey Period: July 2024
Number of Respondents: 125 banking executives responsible for cybersecurity at community and mid-size banks in the United States

Our online survey included questions that explored the following:

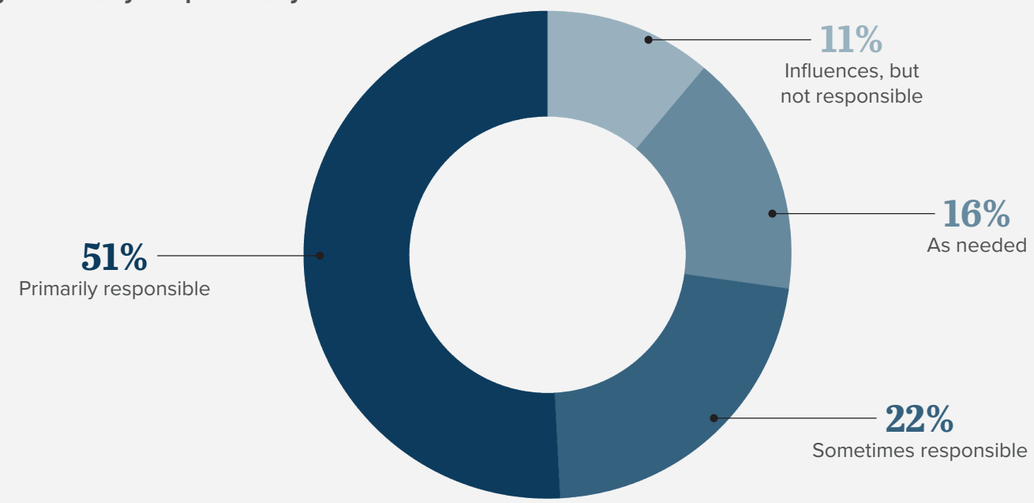
- Attitudes and perceptions toward cyber threats and risks
- History of actual and attempted data breaches
- Threat management and readiness
- Business operations, security training, and audits
- Strategic planning
- Security frameworks (including prevention, response, and reporting plans and policies, and technical platforms)
- Cyber insurance and industry collaboration

Respondent Information

Respondent Role

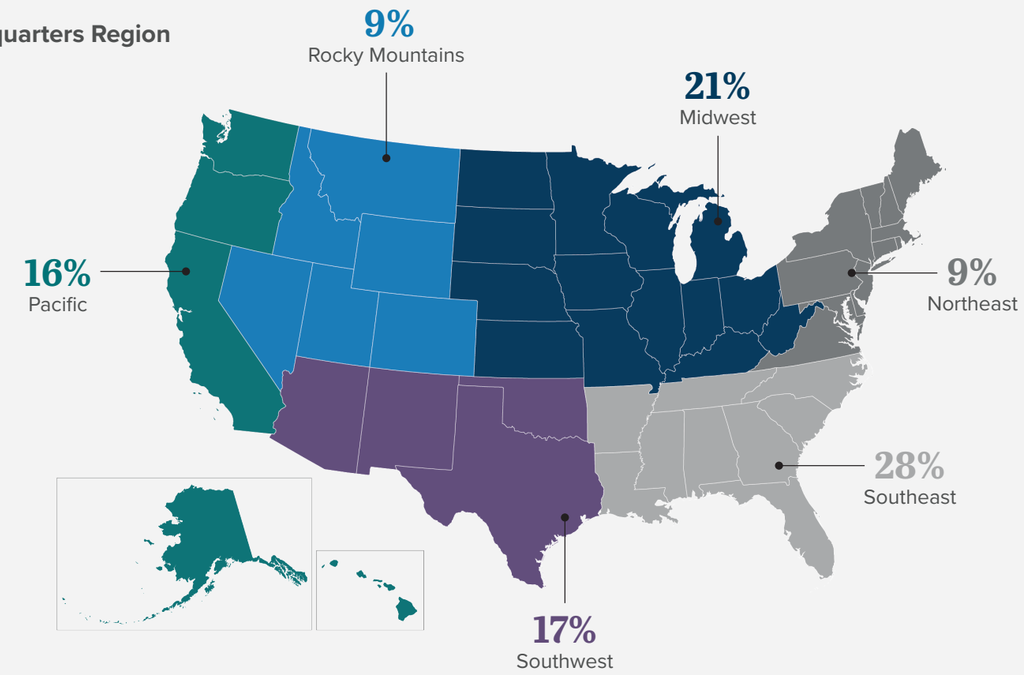


Cybersecurity Responsibility



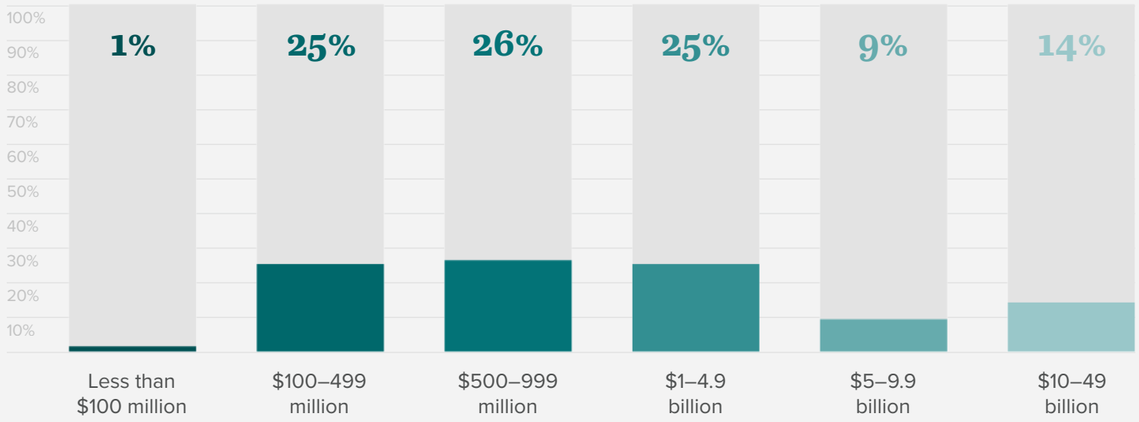
Bank Information

Headquarters Region



Asset Size

Mean is $5.8 billion.

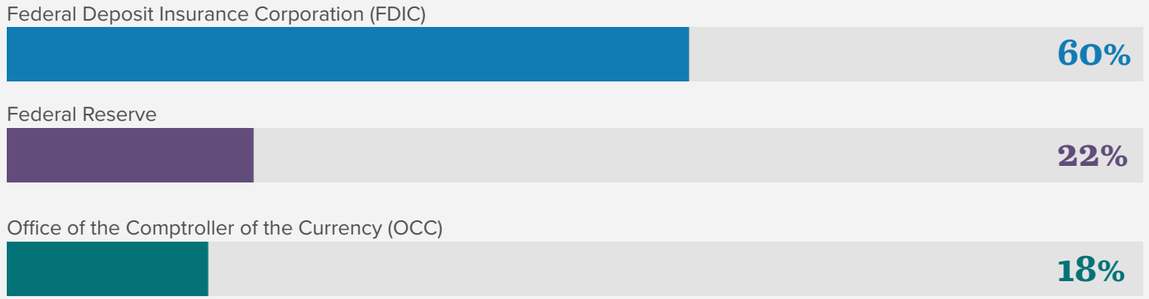


Publicly Traded

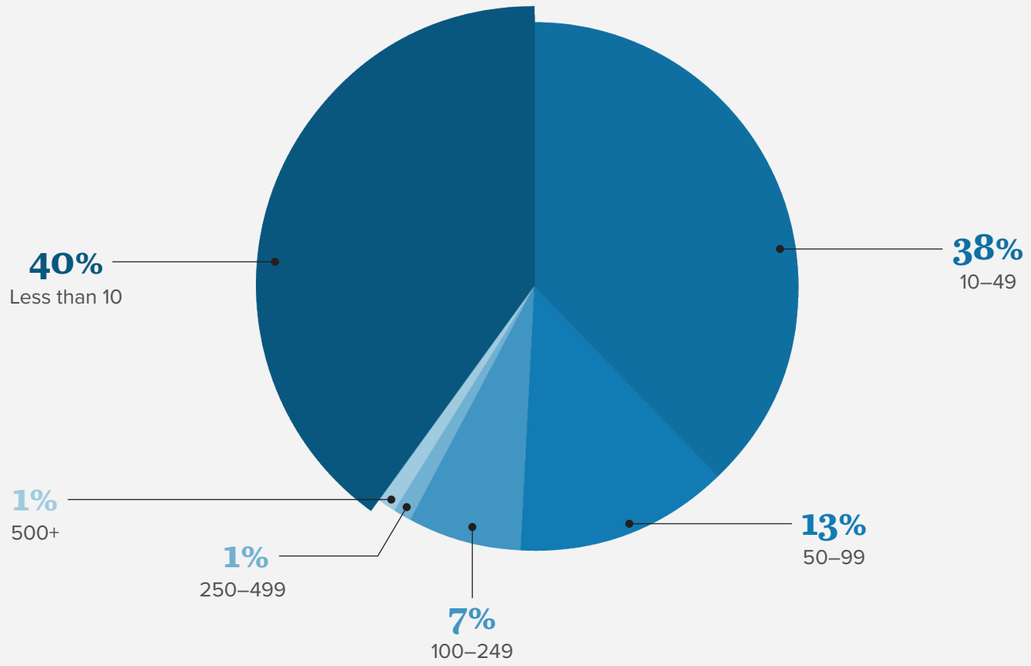
11% Yes

89% No

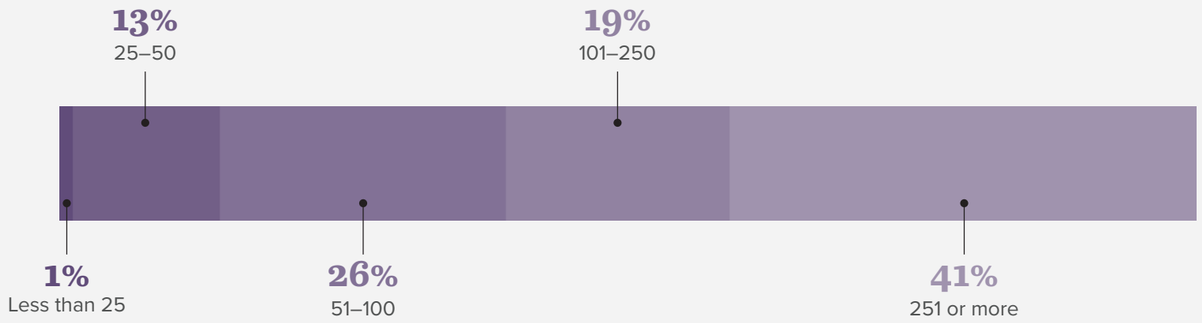
Primary Federal Regulator



Number of Bank Branches



Number of Employees



Cybersecurity:
Leadership from the Top

99%
of respondents have a C-suite executive or other manager whose position encompasses overseeing cybersecurity.

88%
have record retention policies that govern the disposal of data.

88%
plan to increase their cybersecurity budget, with 22% expecting a substantial increase.

Takeaway 1

Post-Incident Regulatory Compliance is Slowly Improving, but Prevention and Preparedness are Lacking

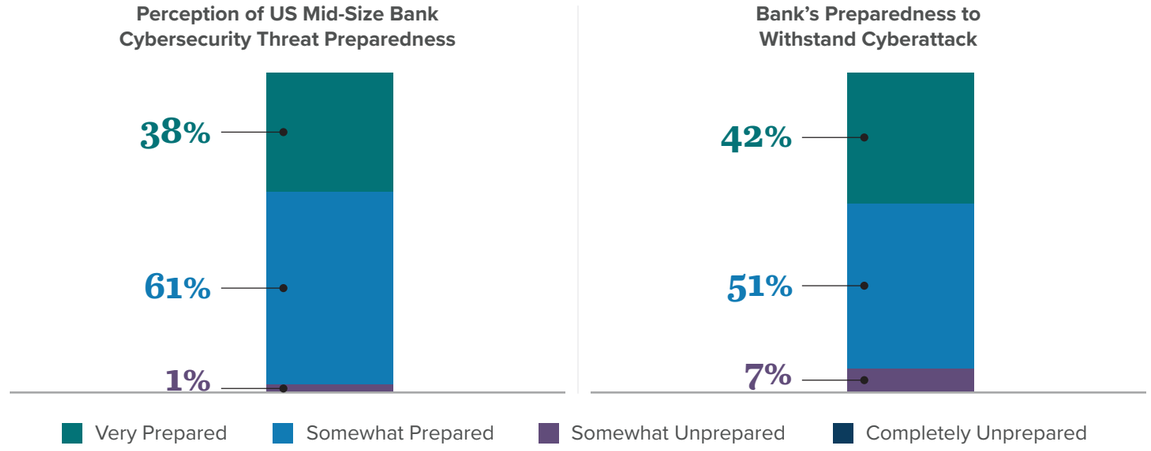
Compared to many other industries, the banking sector is highly regulated. It therefore makes sense that compliance with federal and state data security, data privacy, and data breach laws and regulations is a top priority for banking executives.

By focusing on data breach reporting and other compliance requirements, however, banks are in some respects putting the proverbial cart before the horse. An effective cybersecurity program should be designed to prevent a data breach from happening in the first instance and to limit potential negative impact(s) (resulting from loss of data, customer trust, etc.) and regulatory and law enforcement action(s) in the second instance.

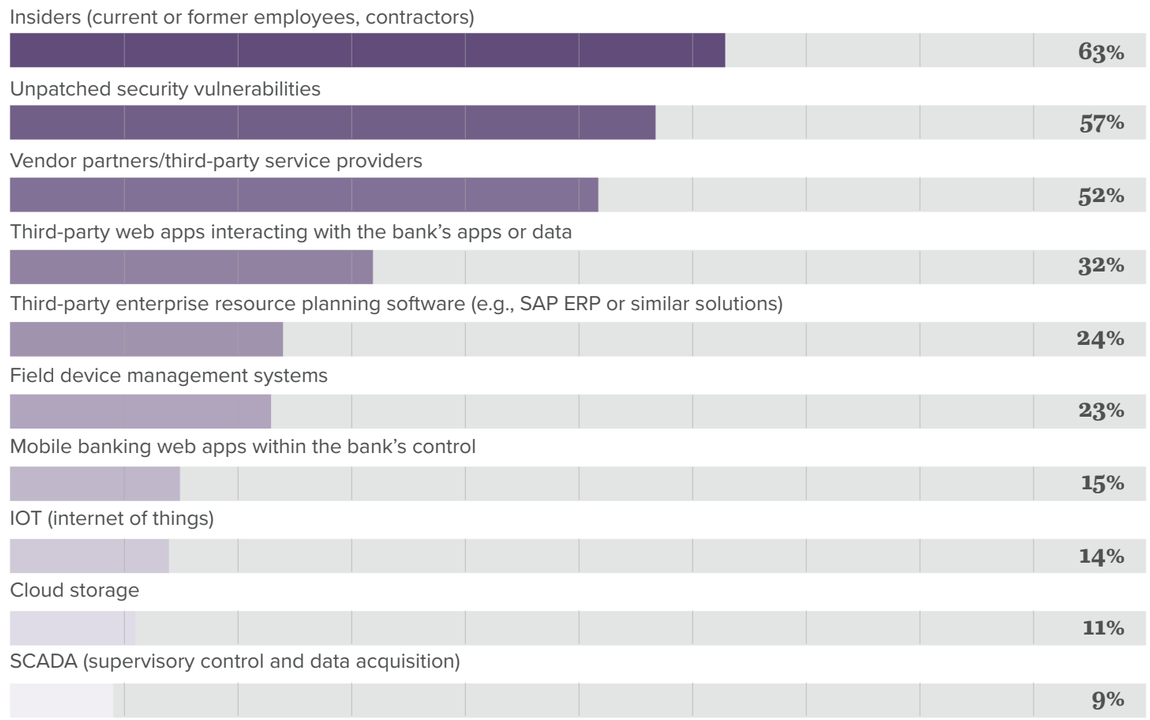
While respondents generally reported a sense of cyber preparedness, their answers to our survey made it clear that there is plenty of work yet to be done.

Cybersecurity Confidence Is Mixed

A solid majority of respondents felt that their own banks and the industry as a whole are prepared to prevent and respond to cyberattacks. Although the general level of confidence is good, only 38% felt that the community and mid-size bank sector was *very* prepared for cyber threats, while 42% felt a similar level of confidence in their own bank's ability to withstand a cyberattack.

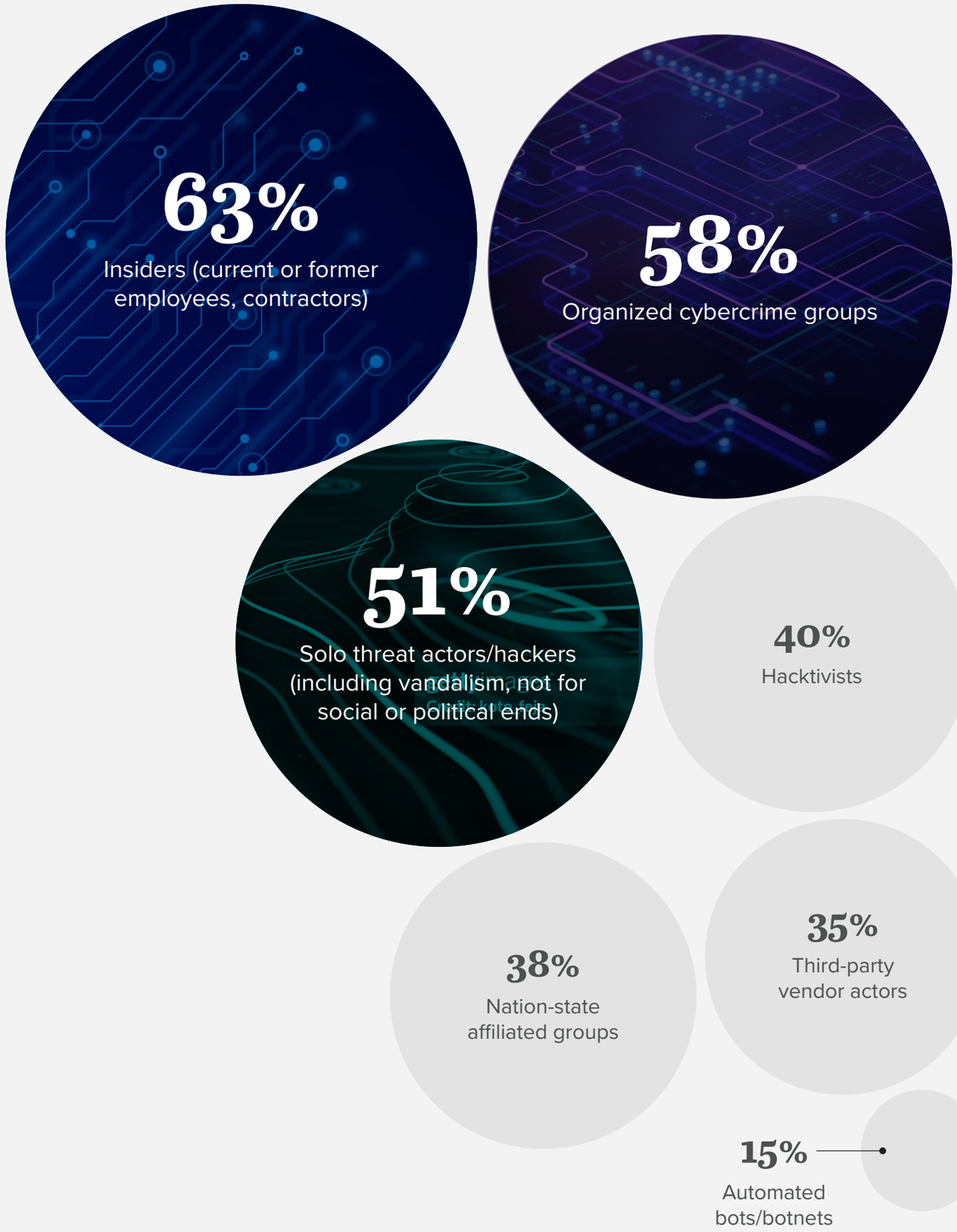


Sixty-three percent of survey respondents identified insiders (e.g., current or former employees, contractors), 57% named unpatched security vulnerabilities, and 52% listed third-party service providers within their perceived top three cybersecurity vulnerabilities. Fewer than one in three respondents included other threats among their top concerns.



An Equally Broad Set of Threat Actors

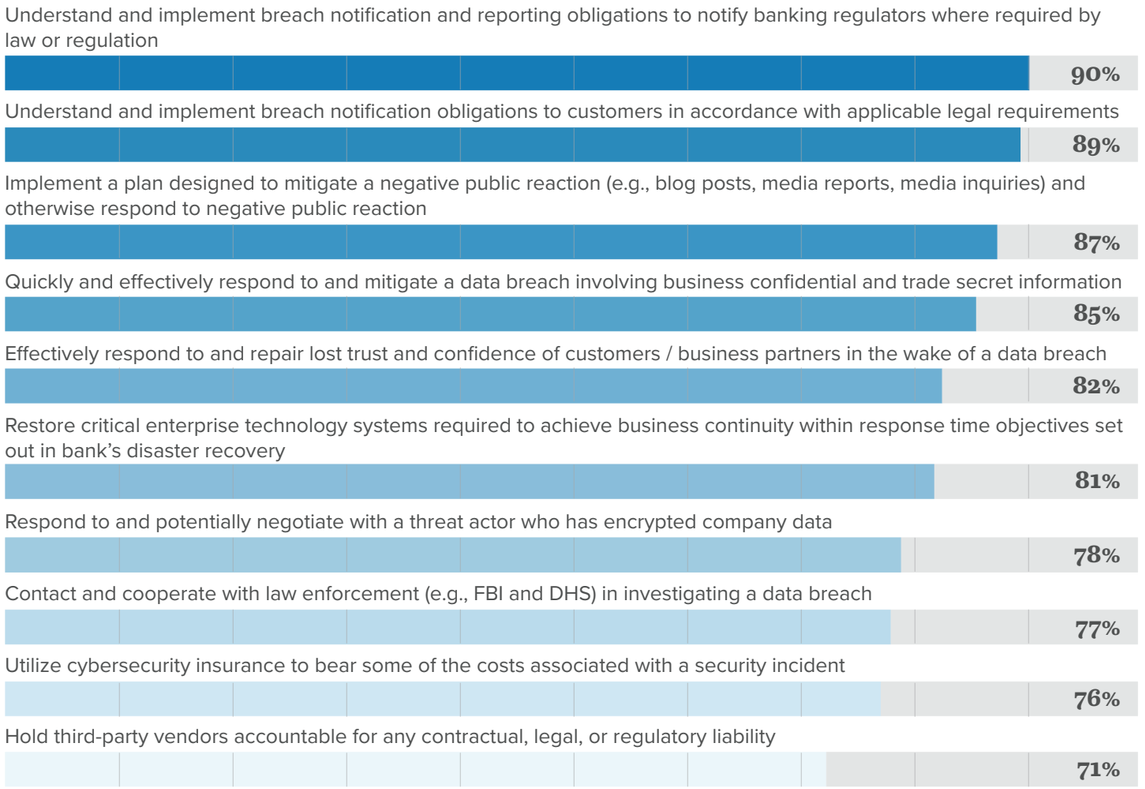
In listing three top perceived threat actors, the majority of respondents identified insiders, organized cybercrime groups, and solo threat actors/hackers.



Ready to Report; Less Ready to Prevent

When asked about their use of specific strategies for responding to a data breach, survey participants reported high levels of engagement across a number of options. Even the lowest-ranked tactic — "hold third-party vendors accountable for any contractual, legal, or regulatory liability" — garnered a 71% positive response rate.

Areas that received the greatest number of affirmative responses tended to involve agency and customer notification requirements following a breach. This is unsurprising because federal law and some state laws generally impose notification obligations on banks in such cases. Notably, as the response strategies moved away from such clearly defined notification requirements and toward more loosely defined actions, such as negotiating with threat actors and cooperating with law enforcement, smaller majorities of respondents indicated that they were prepared to act.

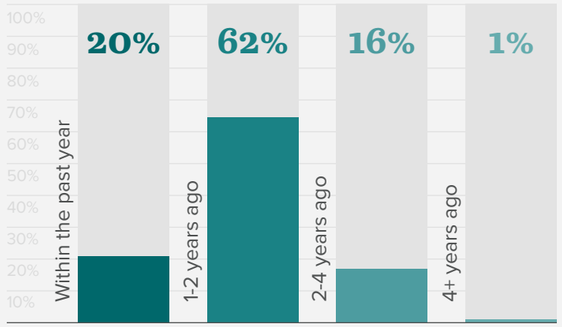


From a breach-prevention perspective, several strategies are used almost universally across respondent banks. These include:

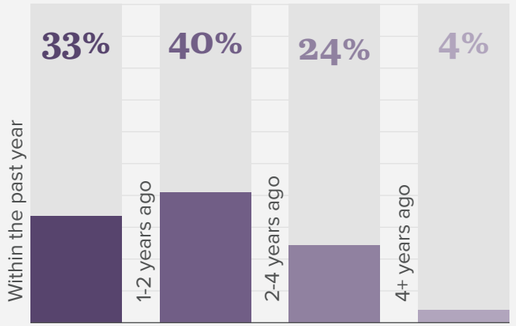
Written Cybersecurity Policies

There is some concern that banks' cybersecurity policies are not reviewed or revised frequently enough to keep pace with evolving technologies and emerging threats (such as AI-specific risks), changing legal and regulatory obligations, and other quality standards. Most commonly, respondents indicated that their bank's written information security policies and IRPs had last been updated somewhere between one and two years ago.

Last Update on Written Information Security Policy



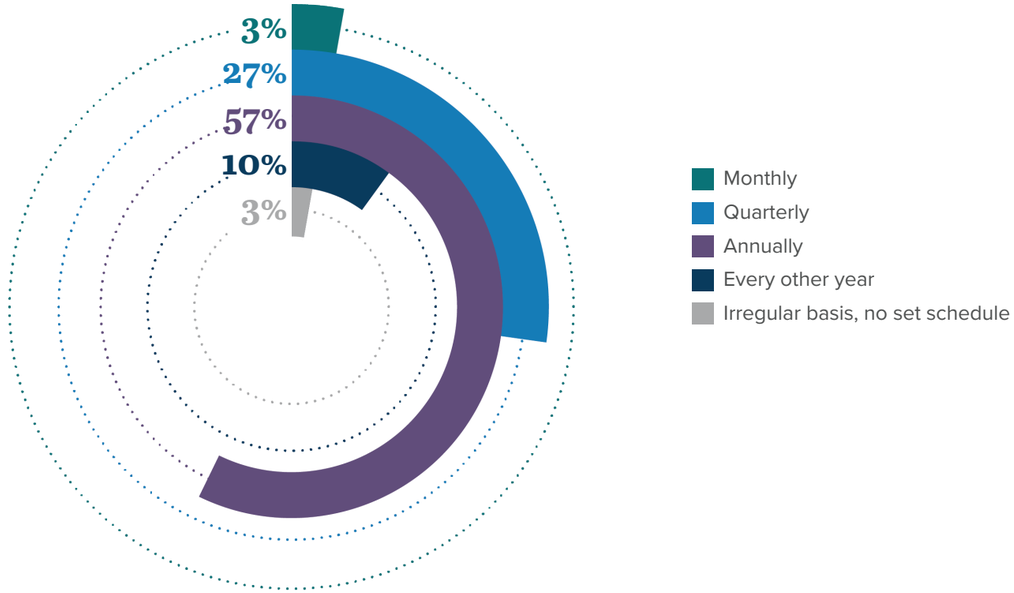
Last Update on Written Incident Response Plan



Training

Ninety-eight percent (98%) of respondents indicated that they conduct cybersecurity training of staff and leadership. More narrowly, 94% reported that they deliver regular education and training to information security staff to enhance their cybersecurity skills.

Encouragingly, training of staff appeared to occur on a regular basis. Eighty-seven percent (87%) of respondents said that their bank provides cybersecurity training at least annually or more often.



Of note, only 5% of banks deliver this training using in-house resources; most rely on third-party providers, government agencies, or industry/trade groups.

Types of Staff Training

82%
Led by third-party service provider

38%
Led by government agency

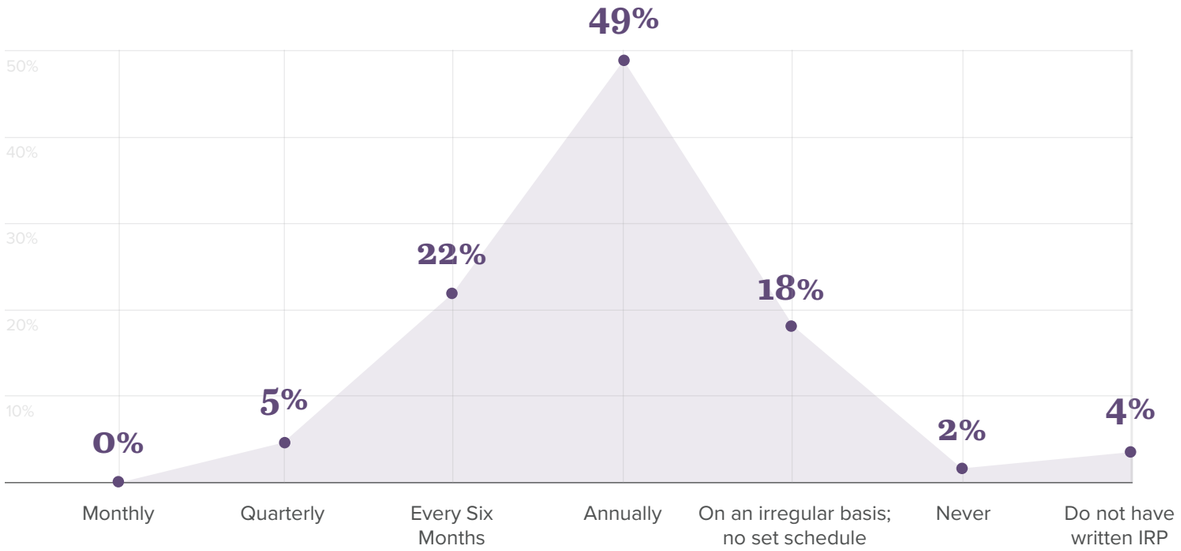
24%
Led by industry/ trade group

5%
Completely in-house

Testing

Tabletop exercises are an excellent way to help organizations prepare for a potential cyber breach by replicating real-world attacks and providing feedback on how well-established plans operated in a simulated crisis event. They can offer key indicators of how quickly and how well leadership and systems are able to respond. As with training, the majority (76%) of survey participants said that their organization conducts tabletop exercises at least annually.

IRP Tabletop Exercises



Penetration testing is another important tool for identifying vulnerabilities. Similar to tabletop exercises, 76% of respondents said that their bank conducts regular cybersecurity penetration testing exercises.

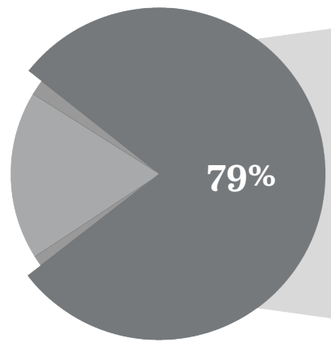
Internal vs. External Penetration Tests

Fifty-six percent (56%) of respondents' banks had penetration tests that revealed specific vulnerabilities. Of such banks, 100% had implemented measures to respond to the vulnerabilities identified in the tests.

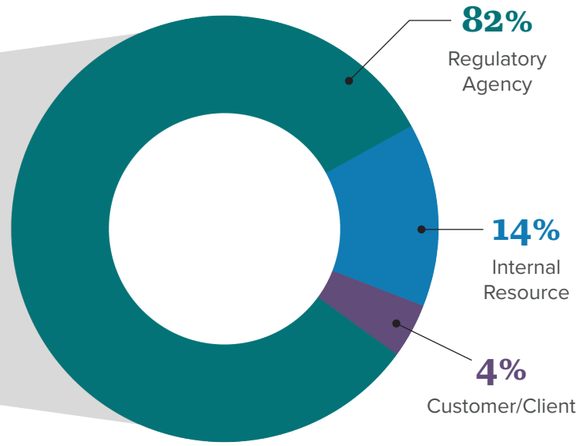
Audits

Among respondents, 90% indicated that their bank conducted external audits of IT/data security area compliance. Of these, 79% conducted a breach readiness audit in the year preceding our survey. The vast majority (82%) of these breach readiness tests and audits were conducted by a regulatory agency.

Has Conducted Breach Readiness Audit in Past Year



Commissioner of Last Breach Readiness or Audit



Areas for Improvement

Although the above responses are encouraging, there are areas in which banks should consider refocusing their protective efforts. In a post-breach scenario, regulatory and law enforcement officials are sure to investigate the cybersecurity practices in place prior to the breach and will be quick to bring enforcement actions against measures found to be inadequate — essentially victimizing the breached bank for a second time.

The Crypto Assets and Cyber Unit of the US Securities and Exchange Commission (SEC), for example, concentrates on bringing regulatory and law enforcement actions against SEC registrants and public companies that lack adequate cybersecurity controls or that fail to promptly and properly disclose cyber risks and incidents. On July 26, 2023, the SEC adopted new rules requiring registrants to disclose material cybersecurity incidents and to report on an annual basis material information regarding their cybersecurity risk management, strategy, and governance.[14]

The *Interagency Guidelines Establishing Information Security Standards* issued by US federal banking agencies requires banks to develop, implement, and maintain a written information security program with administrative, technical, and physical safeguards designed to protect customer information.[15] These regulatory actions underscore the need for community and mid-size banks to develop and implement robust cybersecurity programs, not just to protect company, employee, and customer data but also to limit the likelihood of additional, post-event regulatory scrutiny.

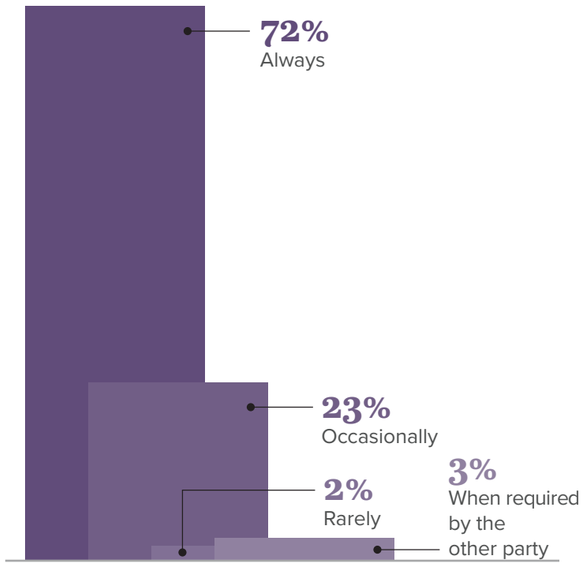
Our survey found that there is room for improvement. For example, while 88% of respondents have written IRPs, only 61% have established a specific incident response team that includes designated team members with clearly assigned roles and responsibilities that are automatically triggered in the event of a data breach.

There seems to be an understandable reluctance for victims of cyber events, including banks, to engage with law enforcement agencies and officials. While there is always the concern that the victim of the breach will become an additional focus of an investigation, cooperation and coordination with law enforcement agencies and officials remain important tools in mitigating the overall impact of a data breach. Seventy-seven percent (77%) of survey respondents indicated that they were prepared to contact and cooperate with law enforcement agencies such as the FBI and the Department of Homeland Security (DHS) following a data breach.

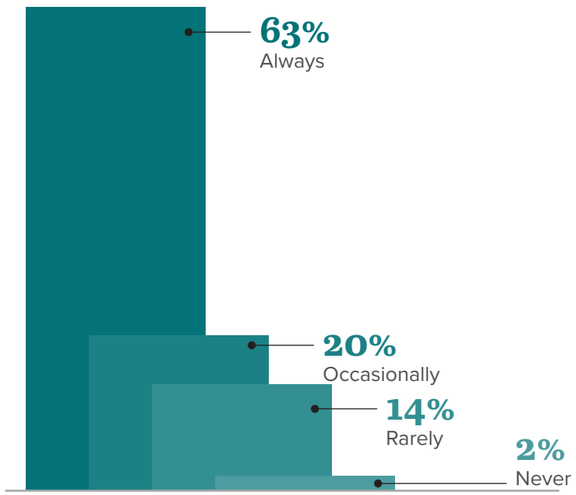
This commitment held true for those respondents who reported that their bank was the victim of a confirmed data breach this past year: 71% confirmed that they had engaged with law enforcement following the breach, and 86% took post-breach action that they deemed successful.

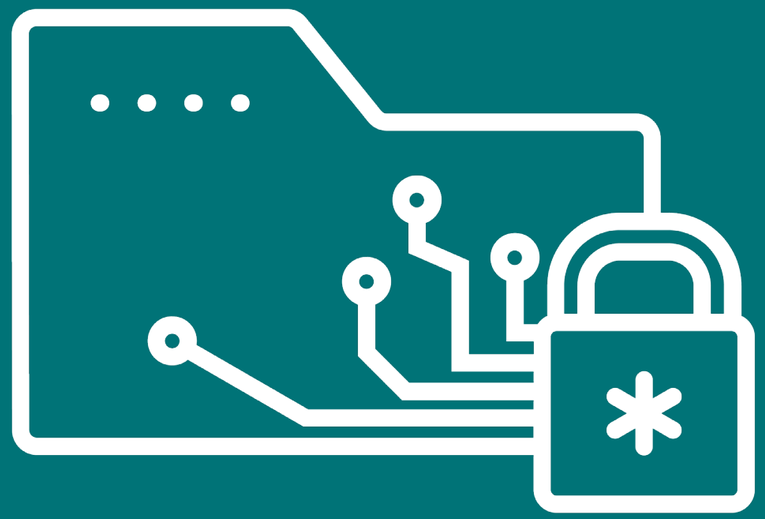
Another area ripe for improvement is encryption. While data management issues that arise in the context of "open banking" may present certain challenges, encryption is a relatively straightforward and well-established tool for minimizing data exposure. Of our survey respondents, only 72% indicated that they always use encrypted communication systems and just 63% said that they use encryption for sensitive information at rest (i.e., stored).

Frequency of Using Encrypted Communication Systems



Frequency of Encryption of Sensitive Information at Rest





Best Practice 01

While community and mid-size banks report relative confidence in their cybersecurity preparedness and indicate that they are taking action to increase their cyber resilience, much more can be done. In particular, **banks should shift some of their attention and resources toward proactive, preventive measures — including testing, encryption, and other low-hanging fruit — that are aimed at preventing and minimizing the impact of a cyberattack**. This is not to encourage noncompliance with breach notification and reporting requirements; rather, it is a call to broaden banks' views of cybersecurity to include the full life cycle and potential costs of cyber threats.

> Cyber breaches have become a common threat to the banking industry; however, cyber awareness and adequate preparedness can increase banks' resilience and mitigate the financial and consumer impact of a breach. The Jones Walker team does a great job of capturing the current state of cybersecurity in community and mid-size banks, as well as outlining gaps in preparedness.

Rhoshunda G. Kelly, Commissioner,
Mississippi Department of Banking and Consumer Finance

Takeaway 02

The Lack of Due Diligence Performed on Third-party Vendors is a Significant Risk

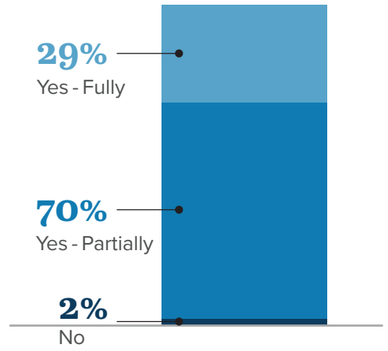
Virtually all (99%) community and mid-size banks rely — in part or in full — on the services of third-party vendors to support their cybersecurity needs. This reliance on outside support is both rational and commendable; in theory, cybersecurity providers have the knowledge and capabilities to provide affordable, effective services to institutions that do not have the amount of resources of national and international banks.

Such relationships, however, do not shift the burden of oversight from bank leadership. Our survey results indicate that banks employ a mixed bag of tools, to varying levels of effectiveness, to ensure that their providers can, will, and do provide the services required before and after a breach.

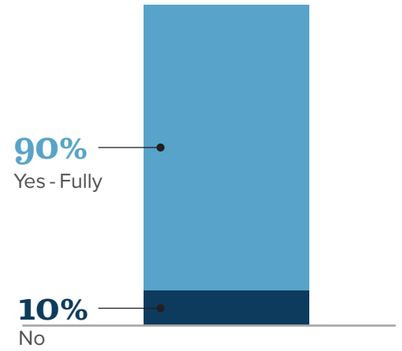
The risks are significant: Verizon's 2024 report found that 15% of breaches involved a third-party or supplier, such as software supply chains, hosting partner infrastructure, or data custodians. For a sector that relies so much on outside vendors, community and mid-size banks must increase their attention on the activities of these parties.

In addition to the 99% of community and mid-size banks that use third-party vendors for cybersecurity, 90% reported using third-party vendors to support open banking, banking-as-a-service, and other fintech platforms.

Contracts With Third-Party Vendors for Cybersecurity



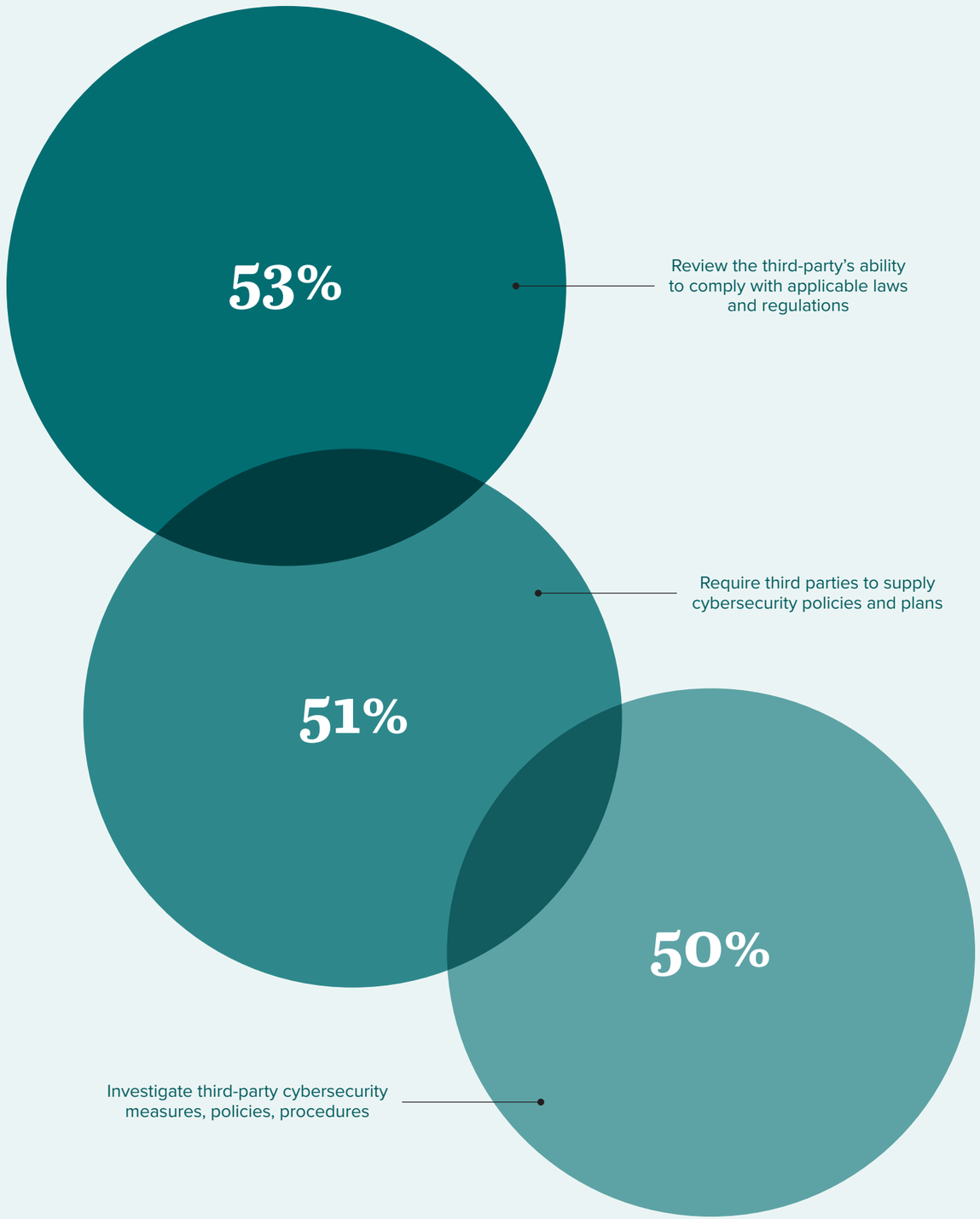
Use Third-Party Vendors for Fin Tech as Banking-as-a- Service



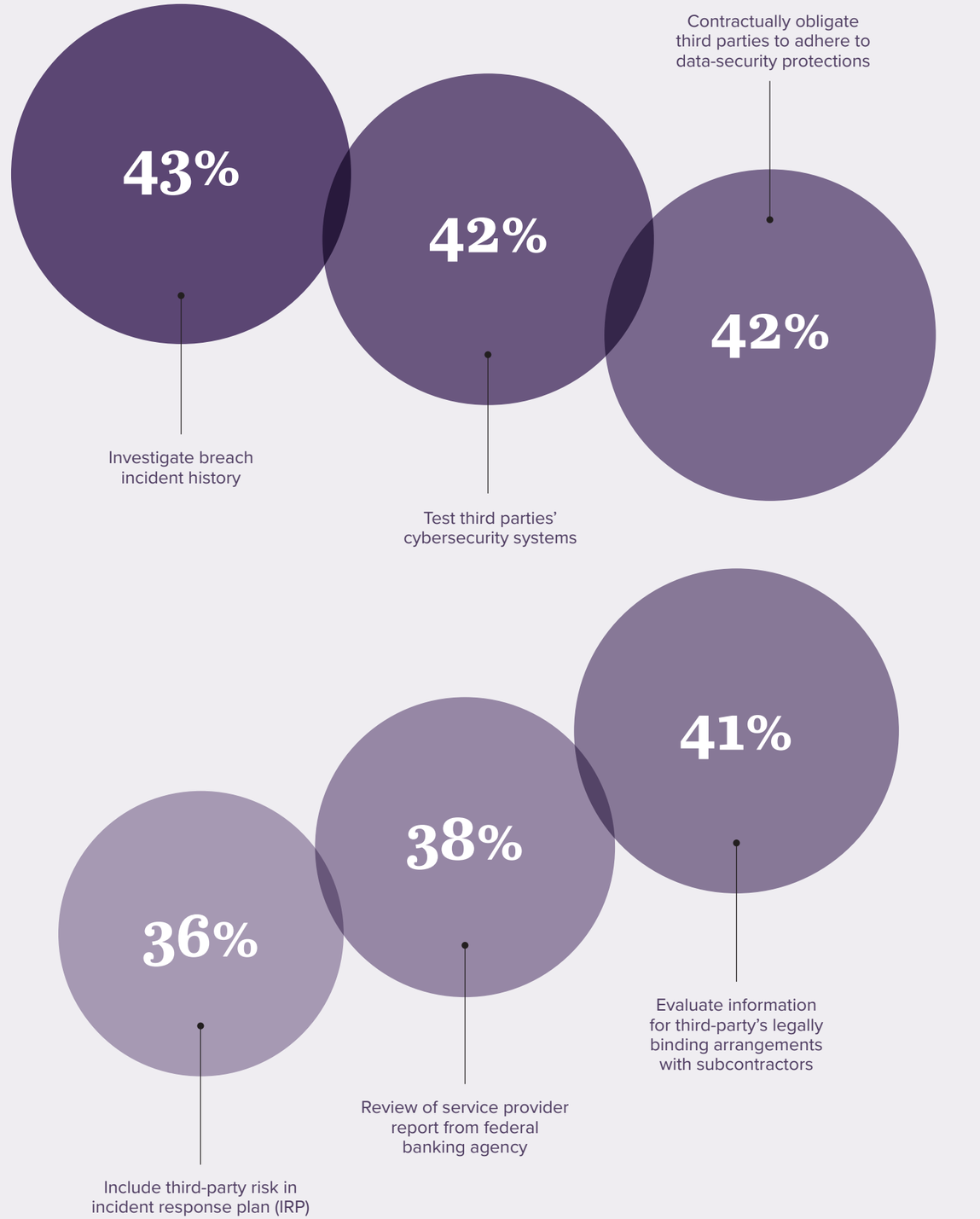
For its part, on October 22, 2024, the Consumer Financial Protection Bureau issued a final rule that will accelerate the shift toward open banking in which, according to the agency, consumers will have more control over their financial data and enjoy additional protections against companies misusing their data.[16] Despite industry misgivings, including concerns that open banking will lead to less secure customer information, the final rule will be effective for the largest depository institutions on April 1, 2026, and will be phased in for all other institutions with more than $850 million in total assets by April 1, 2030.[17]

Most, if not all, community and mid-size banks utilize third-party vendors to provide critical support that necessitates providing such vendors access to sensitive customer data. Conducting initial and ongoing due diligence on third-party vendors involved in high-risk or critical activities and having appropriate cybersecurity risk mitigation measures in place are crucial. However, our survey reflects that banks are lacking in these important areas. While only 1% of our respondents reported that they do not perform such reviews for third-party vendors involved in high-risk or critical activities, there is considerable variation in the level of due diligence conducted, despite many such activities being recommended by federal banking regulators.[18]

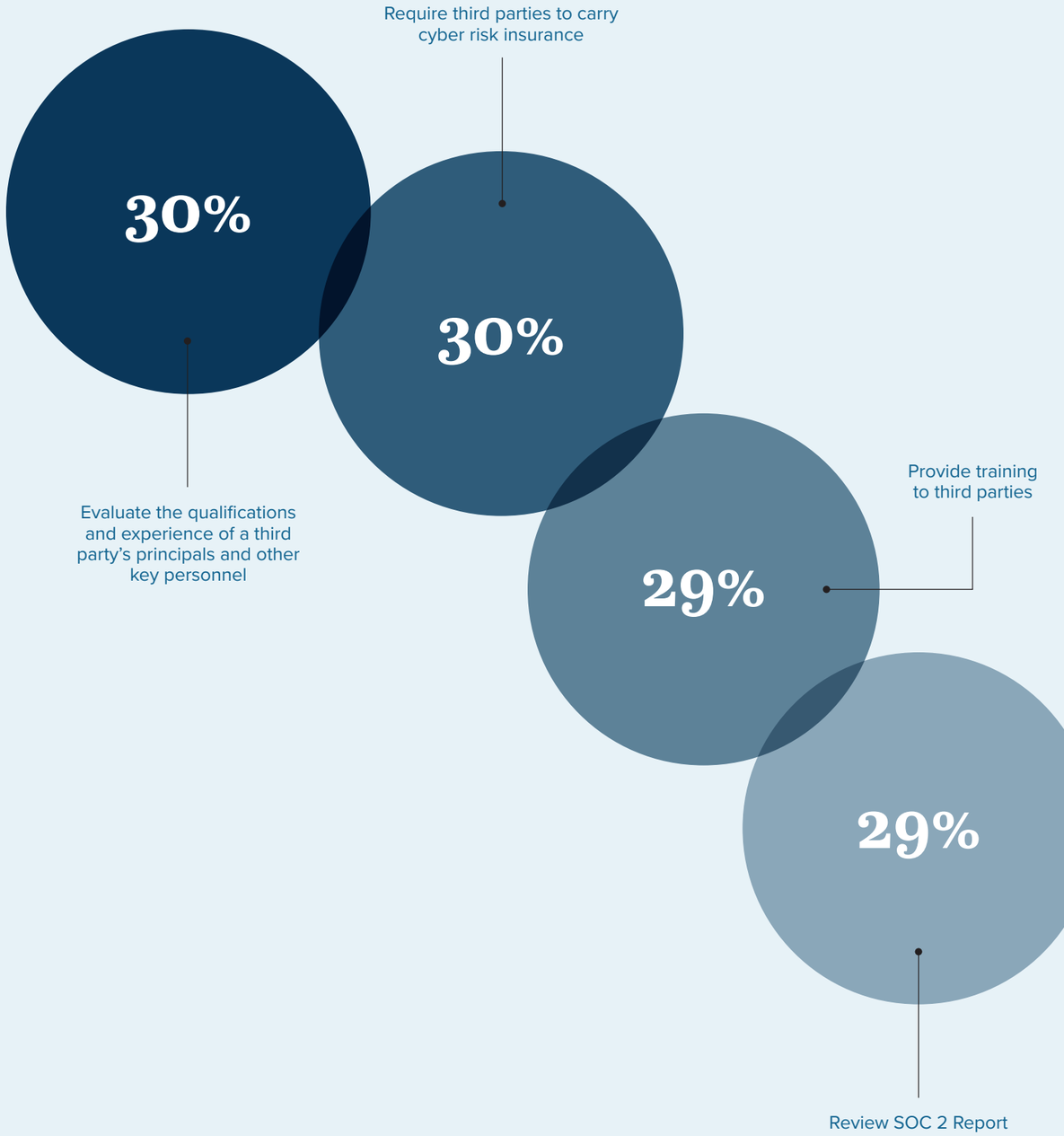
Slightly more than half of respondent banks:

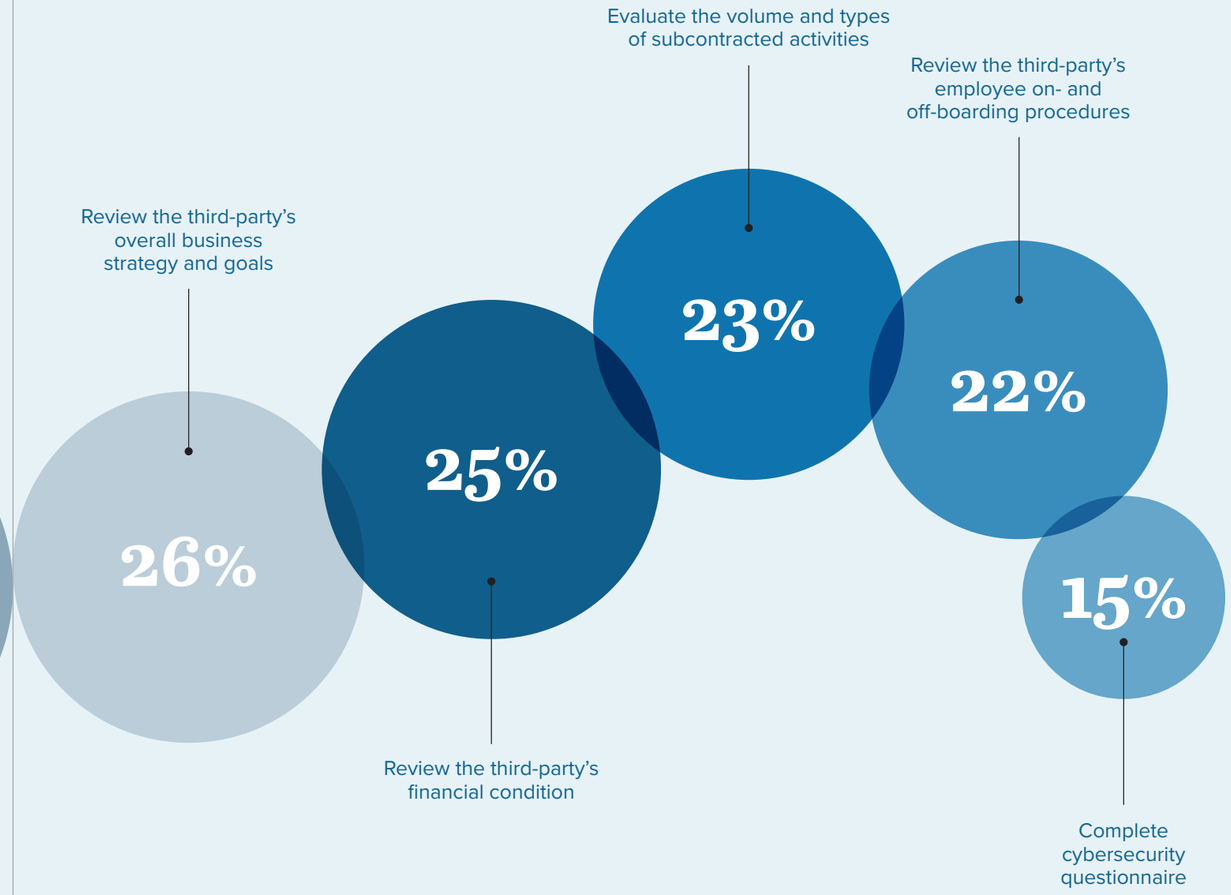


One-third to one-half of respondent banks:



Less than one-third of respondent banks:





1%
We do not perform due diligence regarding sub-contractors' and service providers' security systems

In addition to conducting pre-engagement due diligence on third-party vendors, banks should perform regular, post-engagement monitoring and review of the provider's policies, systems, and security controls. While more than half of the respondent banks review ongoing compliance with laws, regulations, and contractual obligations (62%); third parties' responses to incidents (52%); and audit reports (50%), the respondents' adherence to other expected vendor oversight activities varies widely.

62%
Review ongoing compliance with laws, regulations, and contractual obligations

52%
Review third-party's response to incidents

50%
Review audit reports

49%
Review third-party's response to changing threats and vulnerabilities

42%
Review the volume, nature, and trends of customer inquiries and complaints

41%
Review overall effectiveness of the third-party relationship

35%
Review training provided to employees

32%
Review of the third-party's reliance on, exposure to, and use of subcontractor

30%
Review changes to, or lapses in, the third-party's insurance coverage

23%
Review changes to business strategy and agreements with other entities

23%
Review changes in the third-party's financial condition

19%
Review changes in the third-party's key personnel

Banks should ensure that the responsibilities and activities of third-party vendors engaged in high-risk activities are clearly defined and included in their service contracts. As above, most respondents reported that certain requirements are documented contractually, but the specifics vary considerably.

58%
Require right to audit

50%
Require prompt notification in the event of a data breach

50%
Defined performance measures

50%
Require vendor to maintain security program compliant with federal guidance

46%
Specify type and frequency of reports (financial, security, etc.)

41%
Require performance be subject to regulatory oversight

27%
Required notification of use or intent to use a subcontractor

26%
Require notification of significant strategic or operational changes

25%
Prohibit the use and disclosure of information except as necessary

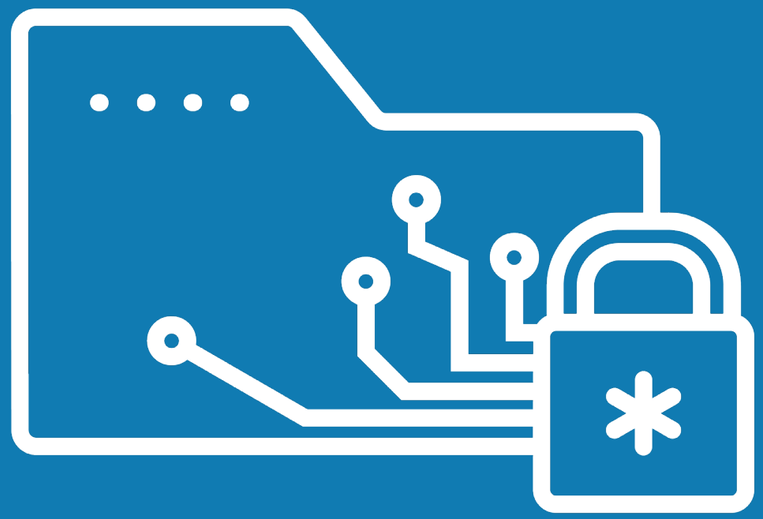
23%
Indication of ownership and license

23%
Indemnification requirement for data breach

23%
Insurance requirements

One very surprising data point is that only 71% of respondents hold third-party vendors accountable for any contractual, legal, or regulatory liability. Equally surprising were our findings that only 23% of respondents require their vendors to indemnify them against claims arising out of a data breach and only 50% require their vendors to promptly notify the bank in the event of a data breach.

Contracts with third-party vendors should have terms that align with banking agency guidelines and industry best practices. These contracts should require vendors to maintain adequate information security programs and include other terms protecting banks in the event of a security breach, including requiring prompt notice from vendors upon a data breach and indemnification against losses arising out of such breaches.



Best Practice 02

An often overlooked but foundational cornerstone of cybersecurity is having robust contracts in place with all third-party vendors. Contracts should specifically set out the services to be provided, the security controls that must be implemented and maintained to protect both bank data and the systems that will process bank data, and robust indemnity and liability provisions to mitigate the bank's risk in the event of a breach related to a third-party vendor. Assessments of threats and vulnerabilities posed by third-party vendors should follow the "trust but verify" model — the bank should have the right to regularly audit or assess a vendor's security practices and to require remediation of any identified vulnerabilities. **Where possible, banks should identify vendor partners with prior experience in and understanding of the banking industry and the associated regulatory landscape.**

> As we navigate an increasingly complex digital landscape, community and mid-size banks are making valuable strides, yet the journey toward true cyber resilience requires further investment in preventive strategies, vendor management, and external expertise. This will be essential to safeguard these institutions and to preserve the trust of their local communities and the broader financial ecosystem. Jones Walker's 2024 Community and Mid-Size Banks Cybersecurity Survey report serves as a reminder and a resource to help strengthen our defenses, protect our customers' data, and ensure we remain resilient against increasingly sophisticated cyber threats.
>
> **Granville Tate, Jr.,** Executive Vice President and Chief Administrative Officer, *Trustmark*

Takeaway 3

Banks Are Underutilizing Outside Counsel and Cybersecurity Expertise

The banking industry is a relationship industry. Whether serving individuals and local businesses or multimillion-dollar companies, community and mid-size banks must earn and keep the trust of their customers.

In the same spirit, banks benefit from working closely and cooperatively with trusted advisors. Outside legal counsel with deep experience in privacy, data protection and cybersecurity law, negotiating contracts with critical vendors, establishing and maintaining compliance and governance programs, and advising on data breach prevention and response is a baseline requirement for institutions seeking to better protect themselves against financial, regulatory, public relations, and other risks.

Banks' attorneys should also have experience working with insurers to effectively identify and negotiate cyber policy terms and collaborating with industry participants and outside experts to share and implement cybersecurity best practices. Consulting with attorneys can also establish attorney-client privilege, helping protect banks in the event of a regulatory or law enforcement investigation or commercial dispute. While beyond the immediate scope of this report, asserting privilege and having supporting procedures in place can be a critical part of implementing an effective IRP.

It is important to emphasize this point: *banks do not need to, nor should they, go it alone*.

> **"(only) 41% of cyber insurance holders have had their policy reviewed to ensure sufficient coverage"**

Cybersecurity Insurance Remains an Important Line of Defense

Despite the fact that insurance cannot prevent a breach from occurring, it can go a long way toward providing community and mid-size banks with the resources they need to address a cyberattack and speed their recovery. The good news for banks is that insurance providers have grown increasingly sophisticated in their ability to match premiums to coverage in a way that is more rational and affordable than in previous years.

Insurers can also share industry best practices with their customers, enabling them to identify key steps that can strengthen their cybersecurity programs and platforms. Additionally, the process of applying for cyber insurance can provide an opportunity to conduct what is, in effect, a cybersecurity assessment, as insurers will give considerable scrutiny to potential insureds' cyber resilience during the underwriting process.

More than three-quarters (76%) of our survey respondents indicated that they rely on cyber insurance to help them bear the costs of a cybersecurity incident. Those who have not yet obtained cyber insurance should seriously consider doing so.

Experienced Legal Counsel and Outside Advisors are Invaluable

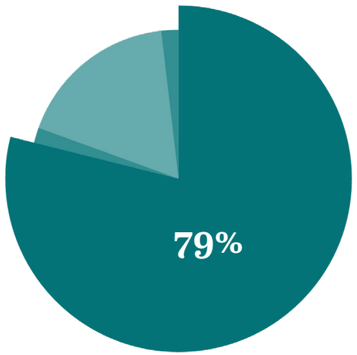
Despite its importance, cyber insurance can be an imperfect solution if not obtained with care and expert advice. Somewhat surprisingly, less than half (41%) of respondents indicated that their cyber insurance policy had been reviewed to ensure that it provided sufficient coverage in the event of a breach. This aligns with respondent reports on their use of outside advisors: only 43% reported using the services of experienced cybersecurity attorneys, and an underwhelming 32% indicated that they use the services of outside pre- and post-incident forensic services consultants.

Of course, outside advisors can provide much more than opinions on cyber insurance terms and pricing, and technological vulnerabilities. Attorneys from Jones Walker and other trusted firms, for example, are investigating and helping clients respond to cyberattacks on a near-daily basis. They are actively involved in government, industry, legal, and other organizations that are focused on cybersecurity issues and data breach prevention and recovery. They are keenly aware of best practices. Given the significant risks posed by threat actors, it is increasingly important to identify and engage effective counsel *before* an attack occurs.

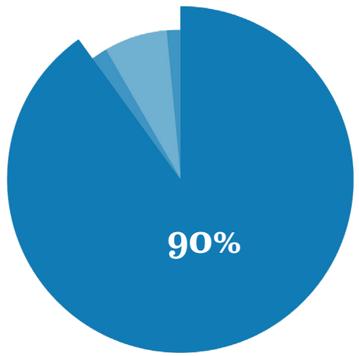
Getting It Right: Banks Emphasize Collaboration

In addition to engaging outside advisors, collaboration with industry partners, government agencies, trade associations, and public-private organizations can help banks identify risks and develop shared strategies to deter threat actors. This is one area in which banks shine; a strong majority cooperate with other banks (79%) and other organizations (90%).

Collaborate With Other Banks to Reduce Cybersecurity Risks

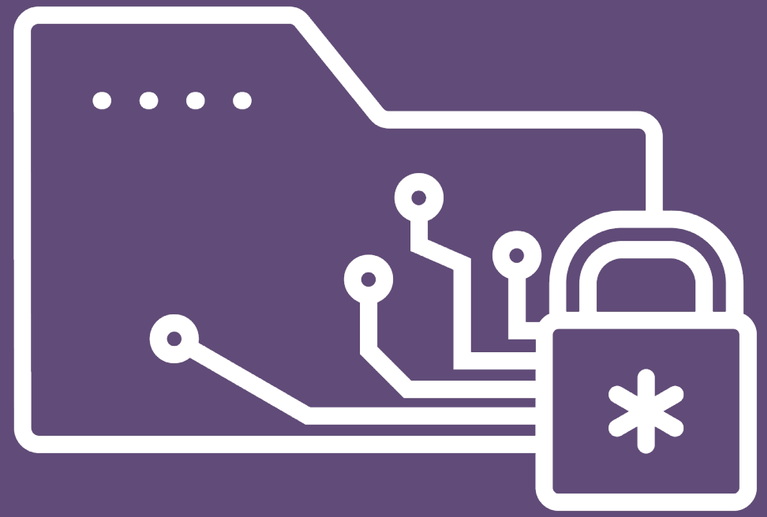


Collaborate With Other Organizations to Reduce Risks To Cybersecurity in the US



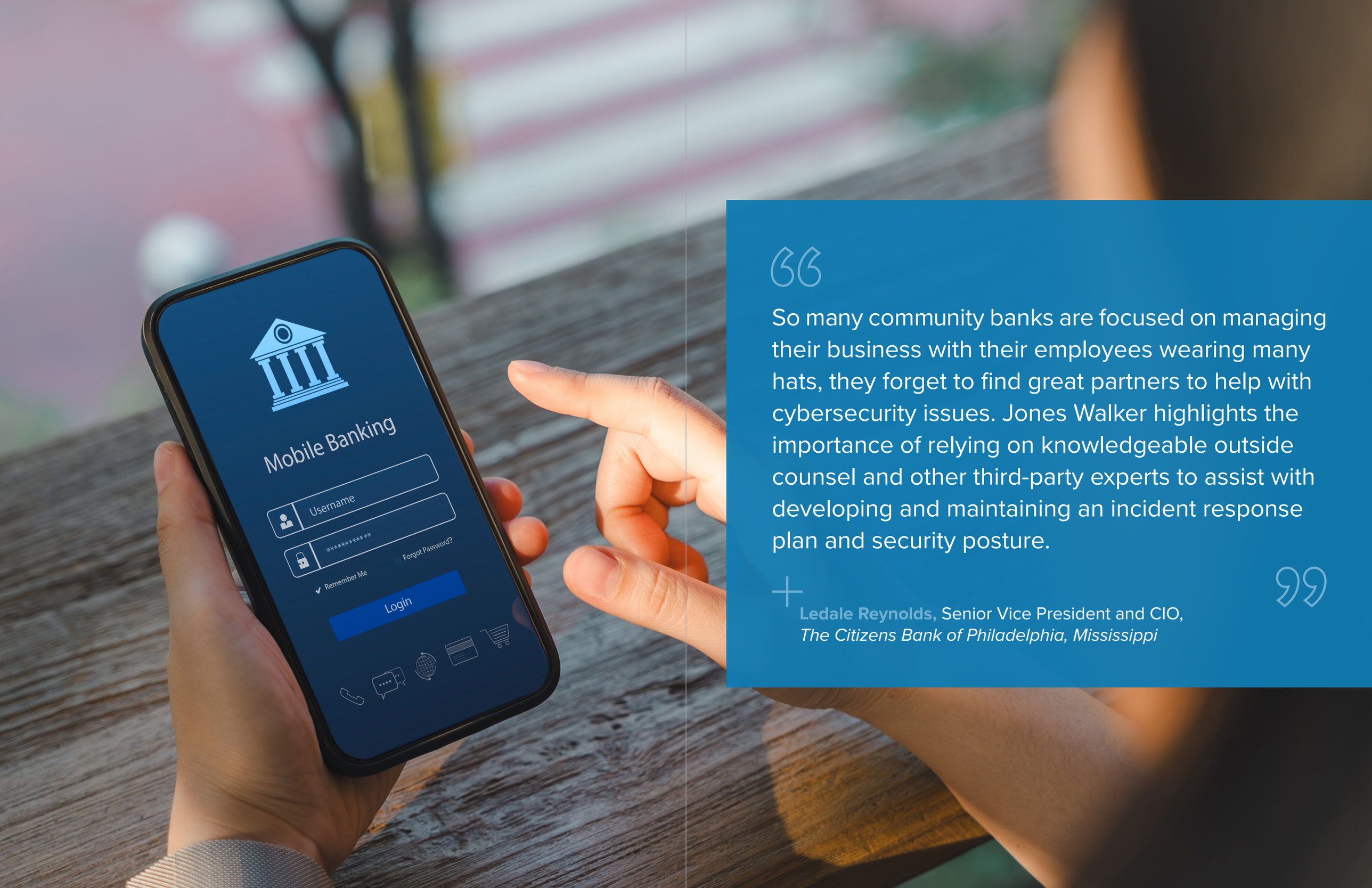
Such groups not only deliver training and resources but also act as a real-time alert service regarding imminent threats and provide strategies and tactics for minimizing risk. Among these is the Cybersecurity Assessment Tool developed by the Federal Financial Institutions Examination Council.[19] This assessment tool provides a repeatable and measurable process designed to help banks and other financial institutions identify their risks and determine their cybersecurity preparedness now and over time.

Of course, the success of any collaborative effort depends on the input and cooperation of all its participants. Community and mid-size banks should ensure that they provide useful information and successes that can help the entire industry.



Best Practice 03

Put simply, community and mid-size banks do not have the resources of their big bank counterparts. At the same time, they cannot afford to put their, and their customers', assets and reputations at risk. **Working with outside consultants, experienced attorneys, and government-, industry-, and nonprofit-led initiatives can help smaller banks direct their resources more effectively without sacrificing cybersecurity protection.**



So many community banks are focused on managing their business with their employees wearing many hats, they forget to find great partners to help with cybersecurity issues. Jones Walker highlights the importance of relying on knowledgeable outside counsel and other third-party experts to assist with developing and maintaining an incident response plan and security posture.

Ledale Reynolds, Senior Vice President and CIO,
The Citizens Bank of Philadelphia, Mississippi

The use of emerging information security technologies, including AI-based platforms, has begun to pay off. In its March 2024 report, *Managing Artificial Intelligence-Specific Cybersecurity Risks in the Financial Services Sector*, the US Department of the Treasury noted that "the adoption of AI technology, including [g]enerative AI, has the potential to significantly improve the quality and cost efficiencies of their cybersecurity and anti-fraud management functions."[20] The report also said that "many financial institutions have incorporated AI-related risks into their existing risk management frameworks, especially those related to information technology, model, compliance, and third-party risk management."

Of particular note to community and mid-size banks, the Treasury stated in its report:

> "With their broader set of client relationships, large [financial institutions] have a wider base of historical fraudulent activity data they can use to develop fraud-detect[ing] AI models. For example, one large firm noted that it developed AI models trained completely on the firm's own internal historical data, which enabled it to reduce fraud activity by an estimated 50%. Fraud activity blocked by such models would likely shift to more vulnerable corners of the sector[,] like smaller institutions that have neither enough data to replicate the larger firms' base data nor the resources to create the systems needed to digest the necessary data."

In other words, as large banks take advantage of AI technologies to reduce cyber risk, that risk is not necessarily disappearing. Rather, it may simply "swim away" to less-protected waters (i.e., community and mid-size banks).

Lastly, the report also sounded an alarm about the industry's reliance on third-party providers of data-driven AI technology: "[I]t is very likely that often[-]overlooked third-party risk considerations such as data integrity and data provenance will emerge as significant concerns for third-party risk management [....] Additionally, the current trend of adopting AI solutions through multiple intermediaries and service providers complicates oversight and transparency."

To help banks navigate this rapidly shifting landscape, the Financial Services Information Sharing and Analysis Center (FS-ISAC) published a *Generative AI Vendor Evaluations & Qualitative Risk Assessment Guide and a Generative AI Vendor Evaluation & Qualitative Risk Assessment Tool*.[21] Further, in its February 2024 report, *Building AI Into Cyber Defense*, the FS-ISAC noted that AI "can automate processes, scan and analyze data, and generate reports — among many other capacities — which saves cybersecurity teams time and greatly expands their scope and impact."[22]

The FS-ISAC identified new developments in AI that can be applied to three specific use cases common to financial services businesses:

1. **Anomaly detection**, in which AI systems are trained to find patterns within complex data structures, allowing them to identify data points that do not conform to accepted patterns. The report highlighted algorithms such as DBSCAN, Isolation Forests, Bayesian Networks, and AutoEncoders as being effective at anomaly detection.

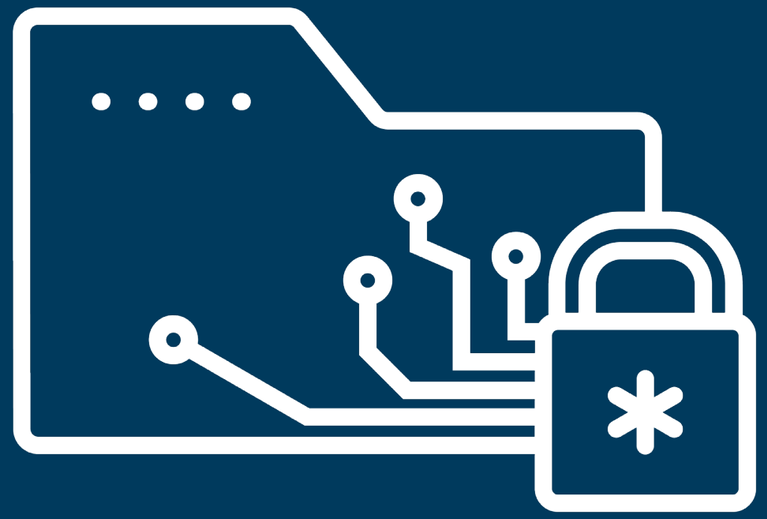
2. **Creating content and structure in unstructured data**, including parsing and triaging long-form text, which simplifies reporting; the extraction of structured data or specific fields that enable, for example, the conversion of information within a threat report into security information and event management queries; the use of phishing simulations, reviewing, and actioning reports; and mapping internal policy and control documentation to achieve operational efficiencies.

3. **Efficient data retrieval**, including converting user descriptions into query language and executing those queries to provide prompt, precise answers. Among other areas, this can provide information on security best practices and controls and identify and prioritize patch management.

Takeaway 4

Responsibly Embracing Emerging Technology Delivers Significant Advantages

Technology solutions, including AI-based tools, are not limited to customer-facing services and internal operational tasks. While banks are understandably cautious about implementing solutions that streamline credit, lending, and other key decisions (that could inadvertently create biases that run afoul of regulations and customer expectations), today's cybersecurity technologies can significantly help community and mid-size banks strengthen their breach prevention and preparedness initiatives without incurring significant costs or creating unforeseen complications.



Best Practice 04

AI can do much more than automate and streamline complex financial, operational, and other tasks. **AI can be a critical driver of cybersecurity, including accounting for and managing the risks associated with other AI solutions.** Resources such as the National Institute of Standards and Technology's (NIST) Cybersecurity Framework[23] and Artificial Intelligence Risk Management Framework[24] can help community and mid-size banks and their third-party vendors identify how to use AI-based cybersecurity solutions to augment existing processes and procedures and close gaps across the cybersecurity life cycle. In developing AI systems, including machine learning and large language models, banks should pay close attention to cybersecurity best practices around data security and extend those best practices to training and test data as well.

> The **2024 Community and Mid-Size Banks Cybersecurity Survey** report is an invaluable resource for our member banks, offering critical insights to help guide our efforts to strengthen cybersecurity. The report highlights key areas that demand our attention, like managing third-party vendor risks and working closely with experienced outside counsel. As the digital landscape continues to grow more complex and cyberattacks become more sophisticated, we must strengthen our defenses by continuously enhancing our cybersecurity protections, ensuring the safety of our institutions.

Scott Latham, President and CEO,
Alabama Bankers Association

Conclusion: Community and Mid-size Banks Should Be Commended — and Commit to Doing More

The majority of cyberattacks are motivated by financial gain. Even when a data breach, distributed denial of service, or ransomware attack is meant as a political or personal statement against a specific entity, the effects of such cyber incidents are almost invariably disruptive and disproportionately costly. The effects of a cyberattack against an entire industry are almost unthinkable.

Given their unique position at the center of local and regional economies and the trillions of dollars in assets and loans they manage, it is no surprise that community and mid-size banks are a prime target for threat actors.

In conducting this survey, we have been impressed by the hard work demonstrated by banking industry participants to develop and strengthen their cybersecurity initiatives. Each of our respondents has made it clear that protecting their customers and their assets is a top priority — their participation in this project is a testament to their commitment, for which we offer them our thanks.

It must be acknowledged, however, that there is room for improvement. Fortunately, there is good news: the majority of cybersecurity strategies do not require banks to reinvent the wheel, and many resources and tools come at comparatively little or no cost.

We hope that you will use this survey to assess your own organization's cyber readiness, identify areas that need attention, and implement tools and tactics that will prepare you to face the full range of cybersecurity threats.

For more information, please contact Robert L. Carothers, Jr.; Andrew R. Lee; Jason M. Loring; Lara Sevener; Thomas E. Walker, Jr.; or your Jones Walker attorney.

Additional Resources

Required Rulemaking on Personal Financial Data Rights, *Consumer Financial Protection Bureau, October 2024*

Global Financial Stability Report: The Last Mile: Financial Vulnerabilities and Risks, Chapter 3: "Cyber Risk: A Growing Concern for Macrofinancial Stability," International Monetary Fund, April 2024

Building AI Into Cyber Defense, FS-ISAC, February 2024

Cyber Fundamentals: Critical baseline security practices for today's threat landscape, FS-ISAC

Financial Services and AI: Leveraging the Advantages, Managing the Risks, FS-ISAC

NIST-AI-600-1, Artificial Intelligence Risk Management Framework: Generative Artificial Intelligence Profile, NIST

Cybersecurity Framework, CSF 2.0 Resource Center, NIST

Managing Artificial Intelligence-Specific Cybersecurity Risks in the Financial Services Sector, Treasury, March 2024

CISA Tabletop Exercise Packages: Tools for stakeholders to conduct planning exercises on a wide range of threat scenarios, Cybersecurity & Infrastructure Security Agency

Cybersecurity Assessment Tool, Federal Financial Institutions Examination Council

Interagency Guidance on Third-Party Relationships: Risk Management, Federal Reserve, FDIC, and OCC, June 2023

Third-Party Risk Management – A Guide for Community Banks, Federal Reserve, FDIC, and OCC, May 2024

Footnotes

[1] *See* https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors/financial-services-sector.

[2] *See* https://www.upguard.com/blog/finance-sector-cyber-attacks.

[3] *See* https://www.experian.com/blogs/ask-experian/moveit-data-breach/.

[4] *See* https://news.bloomberglaw.com/privacy-and-data-security/background-check-data-of-3-billion-stolen-in-breach-suit-says.

[5] *See* https://www.cisa.gov/news-events/alerts/2024/07/19/widespread-it-outage-due-crowdstrike-update.

[6] *See* https://www.imf.org/en/Blogs/Articles/2024/04/09/rising-cyber-threats-pose-serious-concerns-for-financial-stability.

[7] *See* https://www.aba.com/news-research/analysis-guides/banking-snapshot.

[8] *See* https://www.ibm.com/downloads/cas/1KZ3XE9D.

[9] *See* https://www.iansresearch.com/resources/ians-security-budget-benchmark-report.

[10] *See* https://www.verizon.com/business/resources/reports/dbir/.

[11] *See* https://www.paloaltonetworks.com/blog/2024/02/the-power-of-ai-in-cybersecurity/; https://www.weforum.org/agenda/2024/02/what-does-2024-have-in-store-for-the-world-of-cybersecurity/.

[12] *See* GAO-18-644T, Accessible Version, ARTIFICIAL INTELLIGENCE: Emerging Opportunities, Challenges, and Implications for Policy and Research.

[13] *See* https://www.weforum.org/agenda/2024/02/what-does-2024-have-in-store-for-the-world-of-cybersecurity/.

[14] *See* https://www.sec.gov/newsroom/press-releases/2023-139.

[15] *See* https://www.federalreserve.gov/supervisionreg/interagencyguidelines.htm.

[16] *See* https://www.consumerfinance.gov/about-us/newsroom/cfpb-proposes-rule-to-jumpstart-competition-and-accelerate-shift-to-open-banking/.

[17] *See* https://files.consumerfinance.gov/f/documents/cfpb_personal-financial-data-rights_final-rule_2024-06.pdf.

[18] *See* https://www.federalregister.gov/documents/2023/06/09/2023-12340/interagency-guidance-on-third-party-relationships-risk-management; https://www.federalreserve.gov/publications/files/third-party-risk-management-guide-20240503.pdf

[19] *See* https://www.ffiec.gov/cyberassessmenttool.htm; scheduled to sunset on August 31, 2025 per FFIEC announcement.

[20] *See* https://home.treasury.gov/system/files/136/Managing-Artificial-Intelligence-Specific-Cybersecurity-Risks-In-The-Financial-Services-Sector.pdf.

[21] *See* https://www.fsisac.com/knowledge/ai-risk.

[22] *See* https://www.fsisac.com/hubfs/Knowledge/AI/FSISAC_BuildingAI-IntoCyberDefense.pdf.

[23] *See* https://www.nist.gov/cyberframework.

[24] *See* https://www.nist.gov/itl/ai-risk-management-framework.

About the Authors

Andrew R. Lee

D: 504.582.8664
alee@joneswalker.com

Andy Lee is co-leader of the firm's privacy, data strategy and artificial intelligence team and is a partner in the firm's Litigation Practice Group and the corporate compliance team. He advises clients regarding US state and federal privacy and data security requirements, as well as global data protection laws and cybersecurity risks, planning, response, and remediation. Andy is a Certified Information Privacy Professional/United States (CIPP/US), International Association of Privacy Professionals. A trusted resource to the media on the topics of data privacy, cybersecurity preparedness, and data breaches, Andy has been quoted in Bloomberg, the New York Times, the Wall Street Journal, and other publications.

Robert L. Carothers, Jr.,

D: 251.439.7522
rcarothers@joneswalker.com

Rob Carothers is a partner in the firm's Corporate Practice Group and also participates on the firm's privacy, data strategy and artificial intelligence team. He focuses his practice on financial institution regulation and mergers and acquisitions. He also serves as the office head for the firm's Mobile office. Rob works with clients to prepare for regulatory examinations and counsels them on issues that arise during the examinations process. He has assisted bank clients with data privacy issues, including breach response. Rob is a frequent speaker at banking industry conferences and is a member of the Steering Committee for the Auburn University Bank Directors College, serving in this role since its founding in 2010.

Jason M. Loring

D: 404.870.7531
jloring@joneswalker.com

Jason Loring is co-leader of Jones Walker's privacy, data strategy and artificial intelligence team, a partner in the firm's Corporate Practice Group and a member of the commercial transactions team. He advises clients on data privacy and protection, cybersecurity, data governance, breach response, data strategy, and artificial intelligence and machine learning, as well as strategic technology transactions and related commercial matters. Jason is a Certified Information Privacy Manager (CIPM), Certified Information Privacy Professional, United States (CIPP/US), and a Fellow of Information Privacy (FIP), accolades he earned from the International Association of Privacy Professionals (IAPP). Jason's experience, which includes senior leadership positions with global companies, enables him to develop and deliver strategic solutions that help clients identify potential risks and exposure, implement global data privacy and artificial intelligence governance and compliance programs, work with federal and state regulators and law enforcement officials, and respond quickly and effectively to the legal, business, compliance, public relations and other issues that arise in the context of data breaches, ransomware attacks, and other cybersecurity incidents.

Lara Sevener

D: 504.582.8529
lsevener@joneswalker.com

Lara Sevener is co-leader of Jones Walker's Technology Industry Team and is a partner in the firm's Corporate Practice Group and a member of the commercial transactions team. Lara advises clients across all industries with respect to technology-related transactions and strategic commercial contracts including complex software and source code licensing, technology services and development, software as a service, cloud, outsourcing, and digital transactions. Lara is well versed in transactional data privacy and advises clients on the most effective contractual mechanisms to comply with US and international data privacy laws. Lara draws on her experience as in-house commercial, procurement, and technology counsel to provide results-oriented, business-practical legal advice and obtain market-leading positions in the contracts she negotiates.

Thomas E. Walker, Jr.

D: 601.949.4631
twalker@joneswalker.com

Tom Walker is a partner in the firm's Corporate Practice Group focusing on commercial and regulatory matters in the financial services industry, with a depth of experience representing financial institutions. He is also an active participant on the firm's privacy, data strategy and artificial intelligence team. Prior to joining the firm, Tom served as executive vice president and director of a community bank in Mississippi. His experience as general counsel, chief operating officer, chief financial officer, and chief investments officer in the financial services sector enhances his ability to provide legal services advice to his clients.

2024

JONES WALKER

joneswalker.com