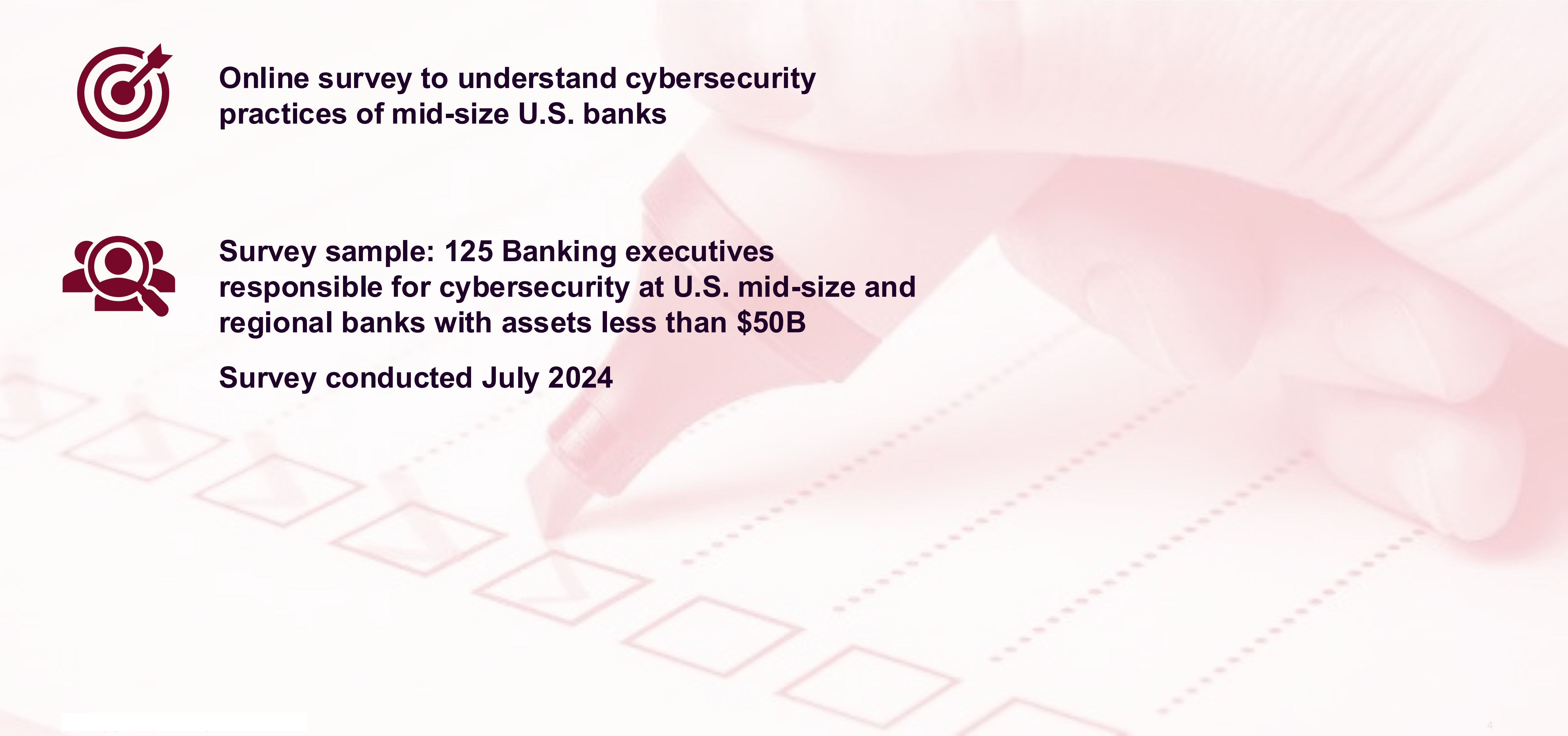
Cybersecurity Market Research with Mid-Size Banks

June 2024

Content

Study Overview

Study Overview



Online survey to understand cybersecurity practices of mid-size U.S. banks

Survey sample: 125 Banking executives responsible for cybersecurity at U.S. mid-size and regional banks with assets less than $50B

Survey conducted July 2024

Summary of Key Findings

Summary of Key Findings

1 Mid-size banks implement initiatives to prevent cyberattacks, but there is room to do more.

- Only 40% feel their bank and is very prepared for a cyberattack.
- Insiders, organized cybercrime groups and individuals are seen as the greatest threat actors, and social engineering attacks are seen as the greatest risk.
- Most do cybersecurity training annually or more often.
- 56% have had a penetration test reveal exploitable vulnerabilities, all of who implemented measures to fix them.
- 80% have conducted a cybersecurity risk audit in the past year, but only 40% reviewed insurance coverage for adequacy.
- Less than three-quarters of banks always use encrypted communication and even less always uses encryption for sensitive information that is stored.

2 Third-party vendors play a big role in cybersecurity for mid-size banks.

- 29% fully use third-party vendors for cybersecurity and another 70% use them partially. Only 2% don't use cybersecurity vendors at all.
- 90% use third-party vendors for fin-tech for banking-as-a-service.
- Nearly all banks perform due diligence on vendors, but they are split on how they do so.
- The most common third-party vendor monitoring is reviewing ongoing compliance with laws and contractual obligations done by 62% of banks.
- The right to audit, prompt notification of a data breach, defined performance measures and complying with information security federal banking guidance are the top requirements for vendors involved in high-risk activities.
- Only 70% hold third-party vendors accountable for contractual liability.

3 6% of mid-size banks have had a data breach.

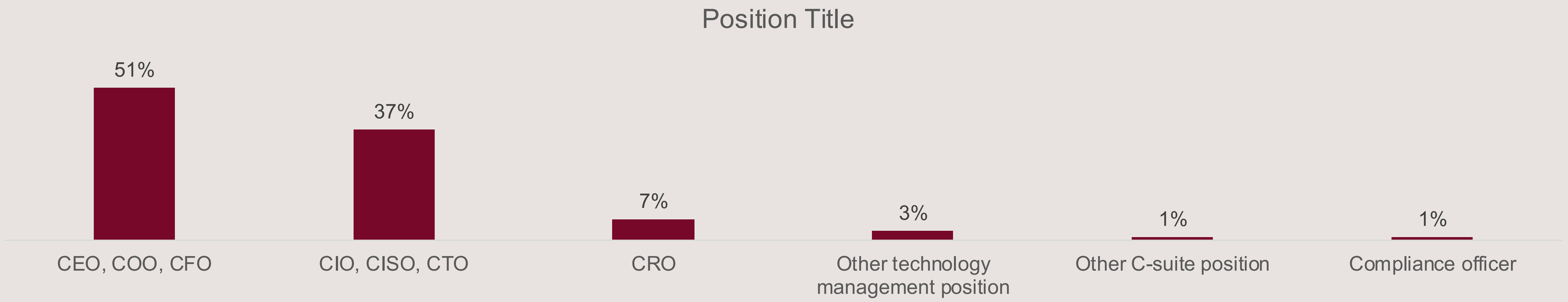
- 4% have had an internal data breach and 2% have had a breach due to an external vendor (7 respondents).
- Another 6% have had an attempted breach.
- These breaches include various types of attacks, most commonly social engineering attacks or account takeovers.
- 2 involved ransomware, both of whom paid a ransom.
- Many different types of vulnerabilities were involved in the breaches.
- 5 engaged with law enforcement and there were various lawsuits filed.
- For 3, total cost of the breach was <$25K and for 3 $25-100K. Only 1 cost $100K+.
- 2 had insurance cover some of the cost and 2 were denied coverage.

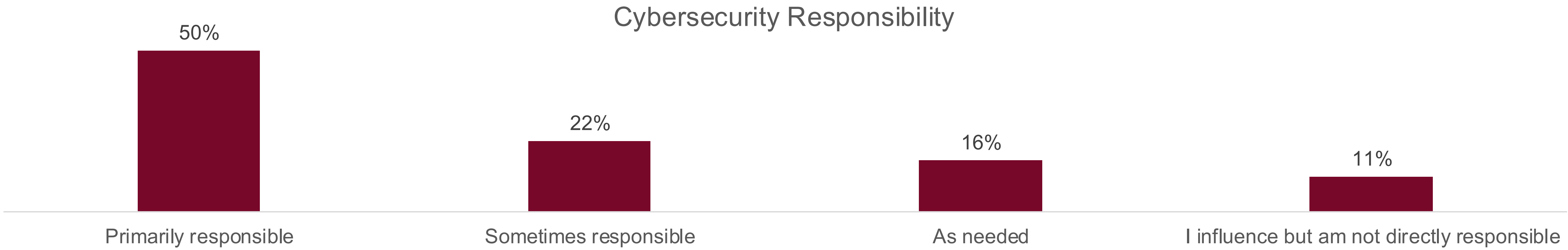
Detailed Findings

Bank Profile

Respondent Role

Half of respondents are CEO, COO or CFO and another 37% are CIO, CISO or CTO. Half are primarily responsible for cybersecurity at their bank.

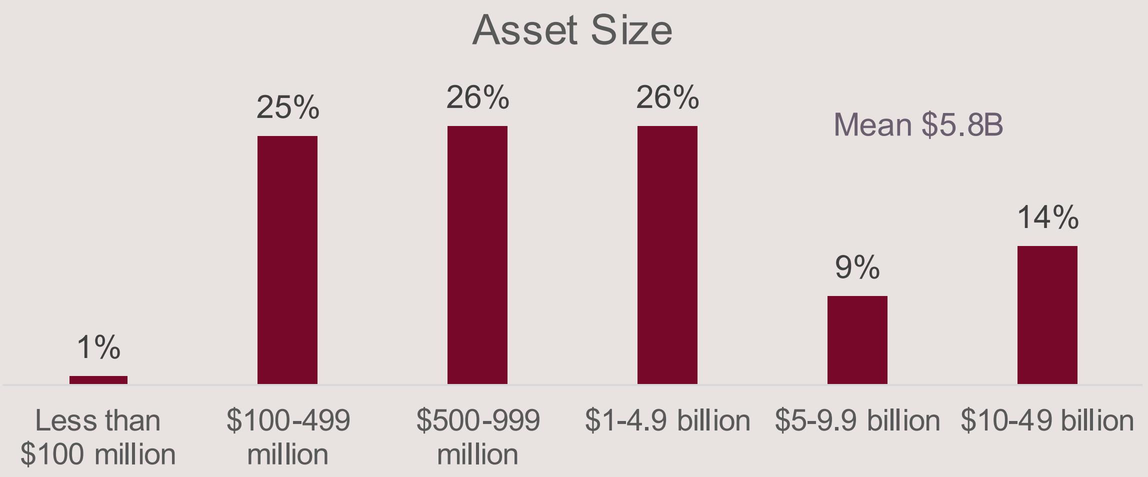


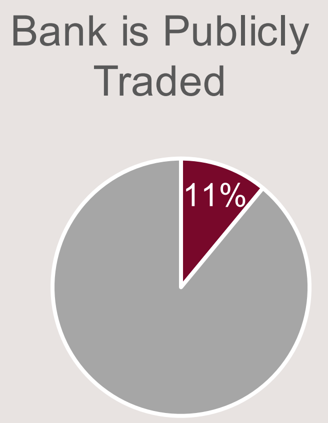


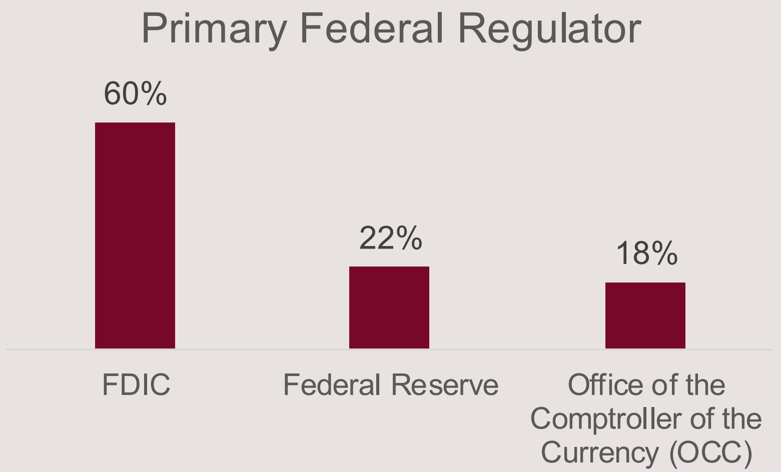
Q4. To what extent are you, in your current role, directly responsible for cybersecurity in the operations at your bank? Q5.Which title best describes your position? (n=125)

Bank Profile

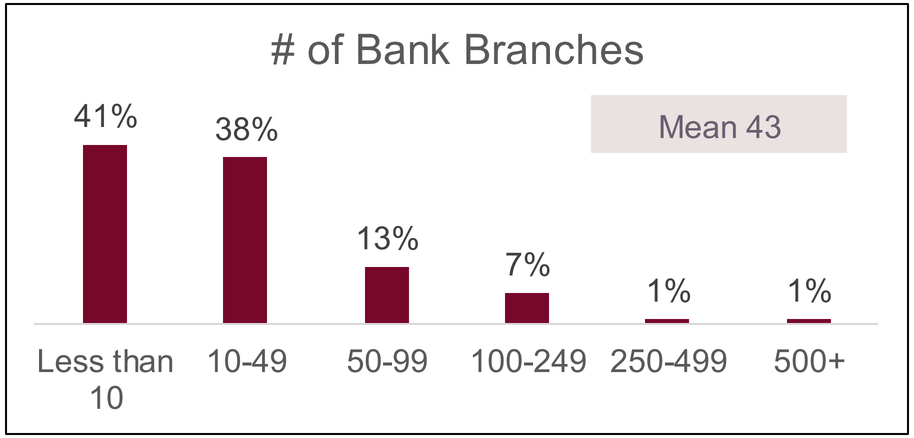
Midsize banks represent a mix of size, asset size and location. 60% are FDIC regulated, and only 11% are publicly traded.

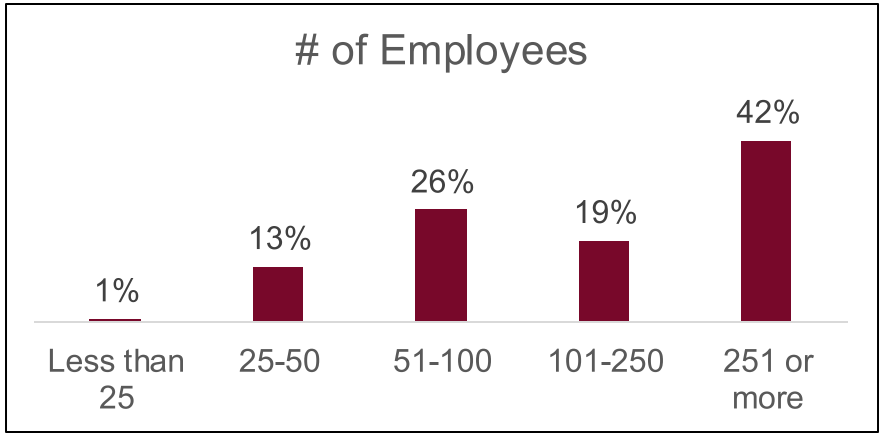






Headquarter Region	
Pacific	16%
Rocky Mountains	9%
Midwest	21%
Southwest	17%
Southeast	29%
Northeast	9%





Q2. In which US region is your bank headquartered? Q3. What is the asset size of your bank? Q6. How many people does your bark employ? Q7. What is your organization's Primary Federal Regulator? Q8. How many branches does your bank oversee? Q9. Is your bank publicly traded? (n=125)

Cybersecurity Profile

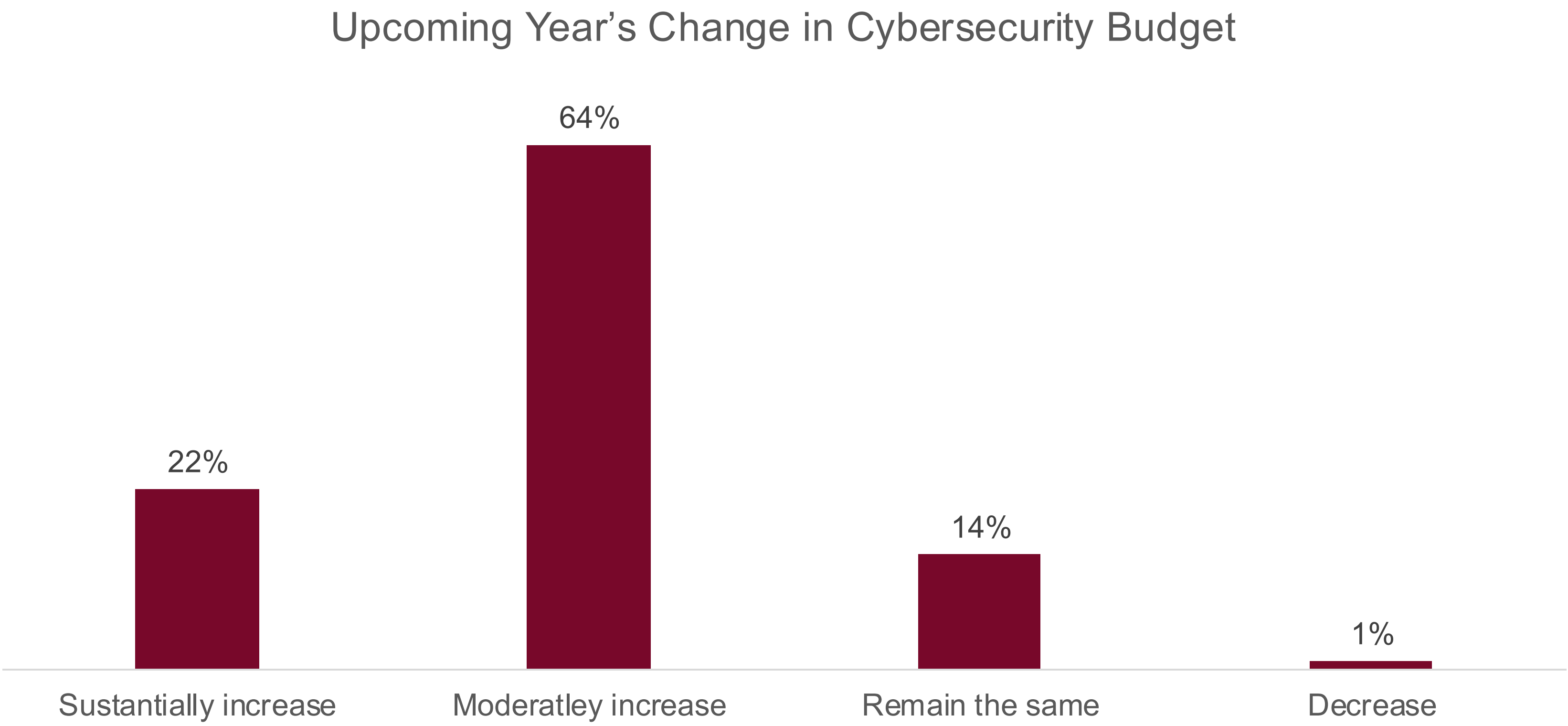
The majority of banks have a management position that encompasses cybersecurity and have retention policies to govern the disposal of data. Most expect their bank's cybersecurity budget to increase in the coming year.

99%

have CISO, CIO, CTO, CRO, CPO or other management position that encompasses cybersecurity

88%

have recorded retention policies that govern disposal of data



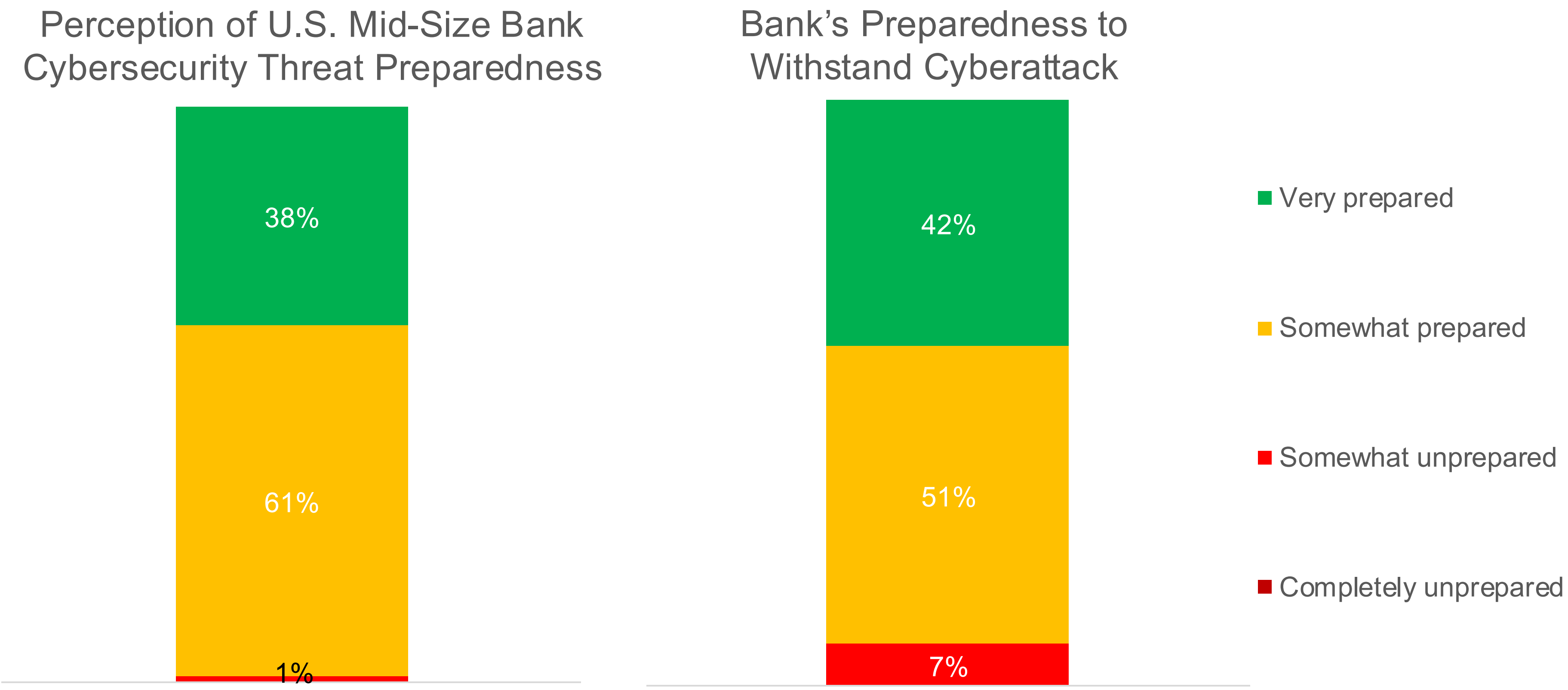
Upcoming Year's Change in Cybersecurity Budget

Q62. How will your bank's cybersecurity budget change in the coming year? Q63. Does your bank have a Chief Information Security Office (CISO), Chief Information Office (CIO), Chief Technology Officer (CTO), Chief Risk Officer (CRO), Chief Privacy Officer (CPO), IT department head or other management position that encompasses cybersecurity, among other management responsibilities? Q65. Does your bank have recorded retention policies that govern the disposal of data related to former customers? (n=125)

Cybersecurity Preparedness

Cybersecurity Preparedness

Roughly 40% feel their own bank and mid-size banks overall are very prepared for a cyberattack. Many feel they are only somewhat prepared.



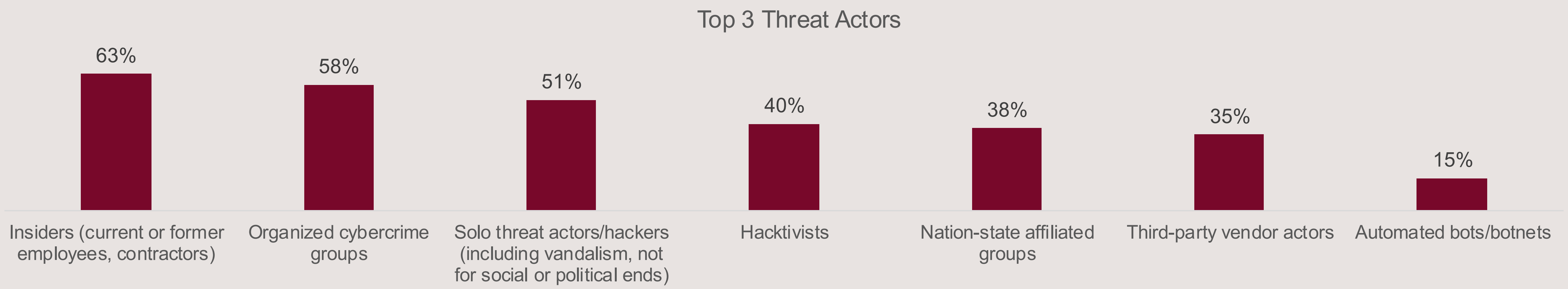
Perception of U.S. Mid-Size Bank Cybersecurity Threat Preparedness

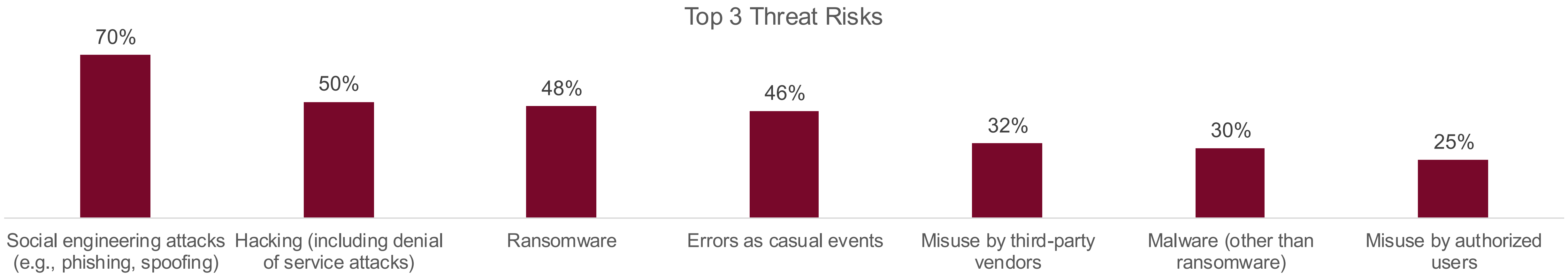
Bank’s Preparedness to Withstand Cyberattack

Q10. How would you describe the overall level of cybersecurity threat preparedness of U.S. community and mid-size/regional banks, based on your experience in the banking industry? Q15. Overall, how prepared is your bank to withstand a cyberattack? (n=125)

Cybersecurity Threats

Respondents see insiders, organized cybercrime groups and individuals as the greatest threat actors, and they see social engineering attacks as the greatest risk.

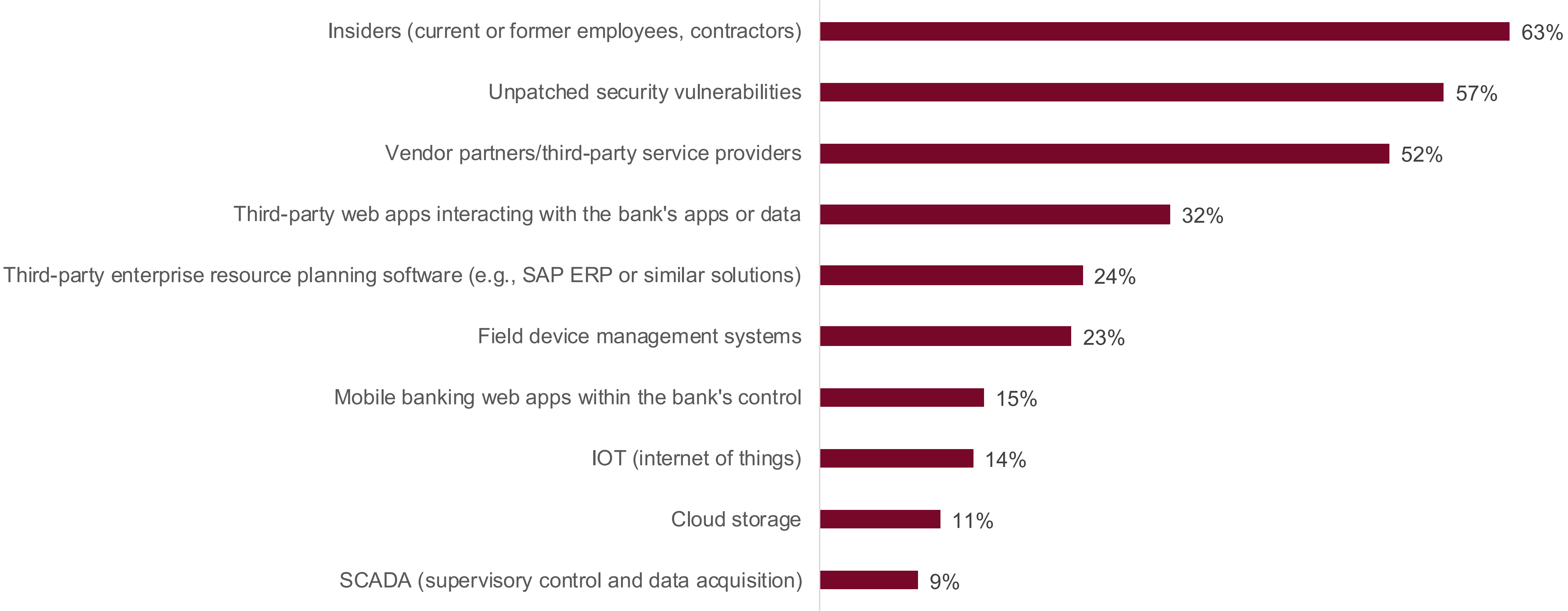




Q12. Please rank your Top 3 leading cybersecurity threat actors targeting U.S. community and mid-size/regional banks. Q13. Please rank your Top 3 leading sources of cybersecurity threat risk to U.S. community and mid-size/regional banks. (n=125)

Cybersecurity Vulnerabilities

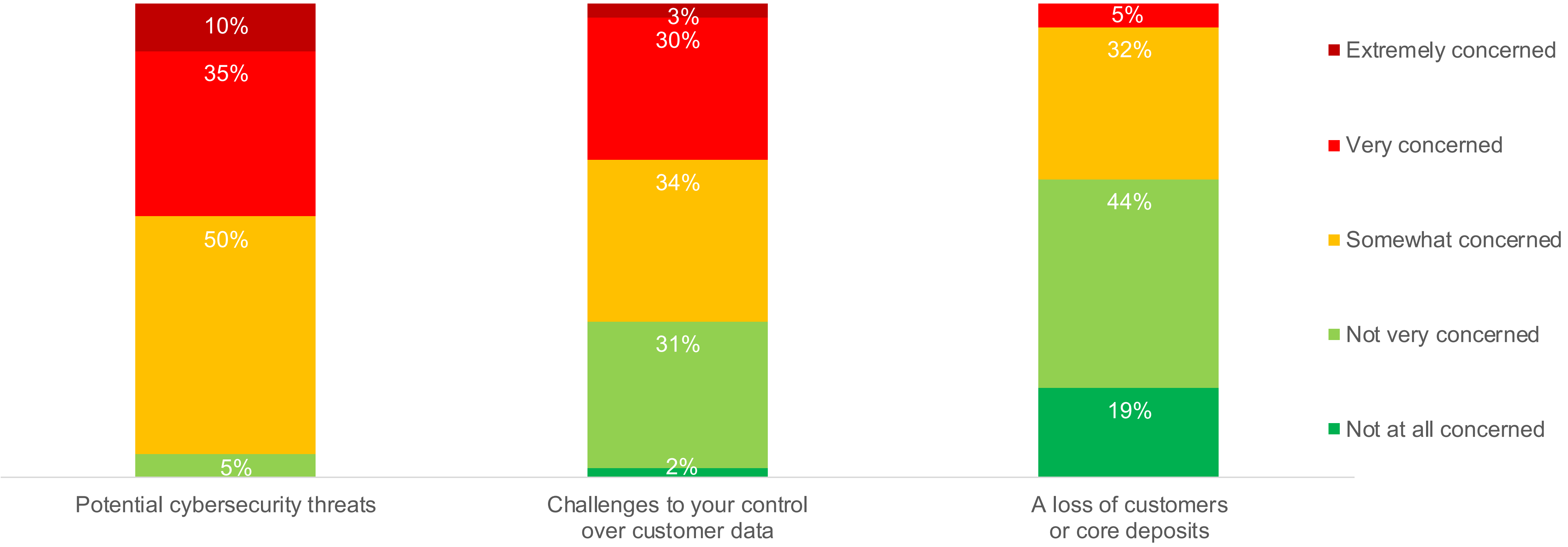
Respondents see insiders, unpatched security and third-party service providers as the greatest cybersecurity vulnerabilities.



Q14. Please rank your Top 3 cybersecurity vulnerabilities of U.S. community and mid-size/regional banks. (n=125)

Concern About Open Banking

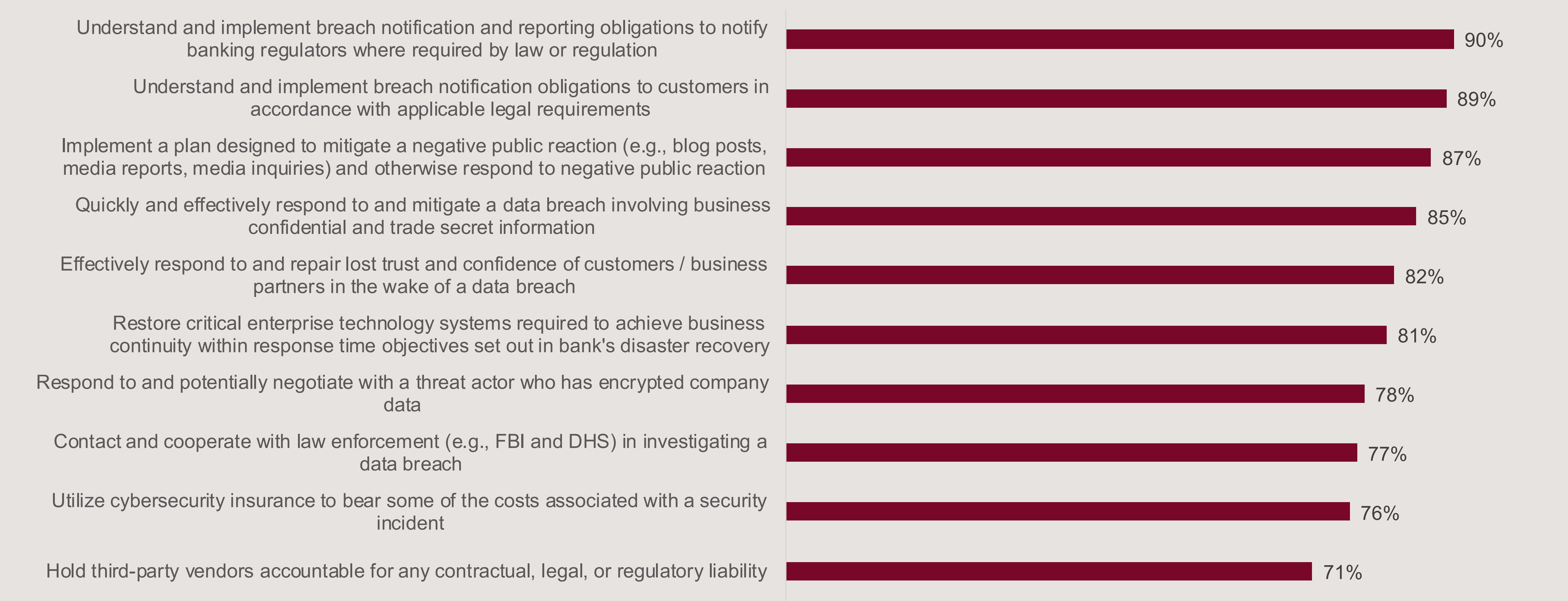
45% are very concerned about potential cybersecurity threats and one-third are very concerned about control over customer data. There is less concern about a loss of core deposits.



Q11. How concerned are you that the implementation of open banking will result in each of the following? Open banking refersto the use of APIs to share financial data and services with third parties. (n=125)

Preparedness for Data Breach

90% of banks implement breach notification obligations to regulators and customers. But only roughly three-quarters use cybersecurity insurance or hold third-party vendors accountable for contractual liability.



Q16. How much do you agree or disagree with each of the statements below regarding your bank's preparedness in the event of adata breach? (n=125)

Implemented at Bank

Strong password requirements for internal authorized user access	100%
Firewall, intrusion detection and prevention systems	100%
Written policies and procedures addressing cybersecurity preparedness and information security	99%
Policy managing, implementing, and cycling software patch updates	98%
Cybersecurity training of staff and leadership	98%
Multi-factor authentication for internal authorized user access	98%
Restricted use of unsupported software	97%
Requirements for internal authorized users to change passwords at specified intervals	97%
Restricted use of personal mobile devices to access the bank's network	96%
Third-party security risk management program	96%

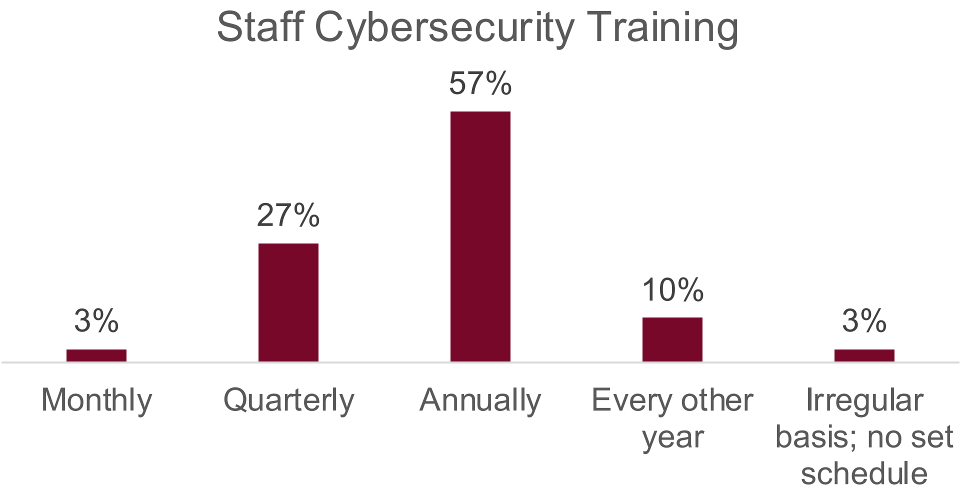
Backups segmented offline, cloud, redundant	95%
Regular education and training for information security staff to enhance cybersecurity skills	94%
Written breach readiness review	92%
Signature-based anti-virus and malware detection	90%
External Audit of IT/data security area compliance	90%
Internal controls/access controls	89%
Written incident response plan (IRP)	88%
Active logging and retention	85%
Encryption of sensitive and air-gap hypersensitive data	84%
Background checks specifically for new hires involved in IT and security functions	82%

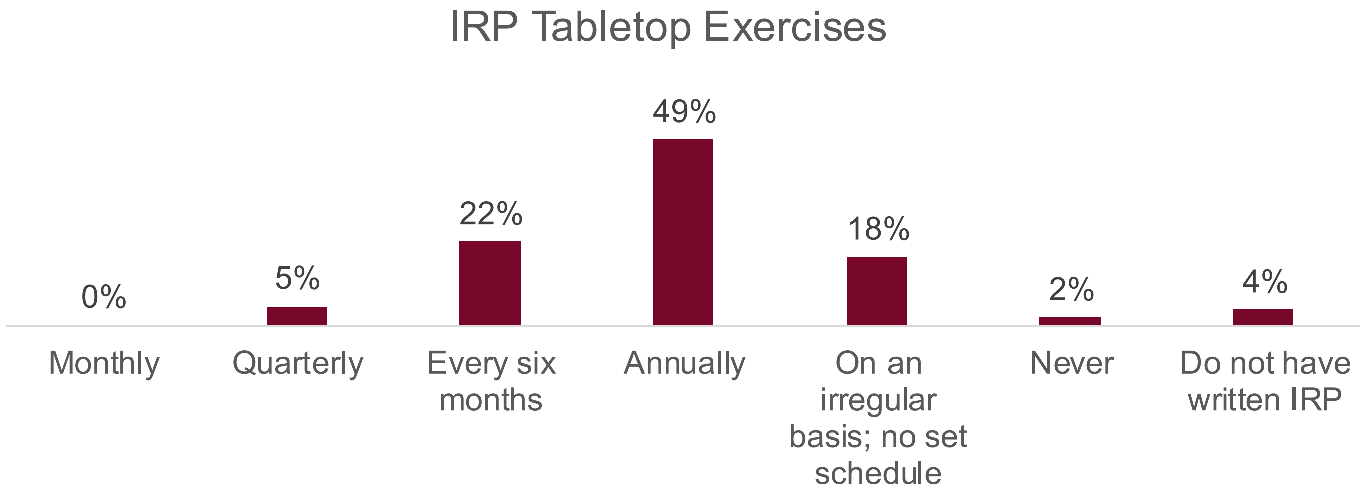
Post-incident communications and/or public relations plan	81%
Regular cybersecurity penetration testing exercises	76%
Managed services provider (MSP) or managed security service provider (MSSP)	73%
Regular cyber-breach tabletop exercises	70%
Cyber or network-risk insurance	68%
Testing that includes mock technology failure exercises	66%
A cybersecurity threat risk assessment developed in accordance with the FFIEC Cybersecurity Assessment Tool	63%
Incident response team with identified team members, roles and responsibilities established	61%
Outside cybersecurity legal counsel	43%
Outside pre- and post-incident forensic services consultant	32%

Q17. Which of the following are implemented at your bank? (n=125)

Cybersecurity Training

Annual cybersecurity training and tabletop exercises are most common. Most training is led by a third-party provider.





Types of Staff Training

Led by third-party service provider
82%

Led by government agency
38%

Led by industry/ trade group
24%

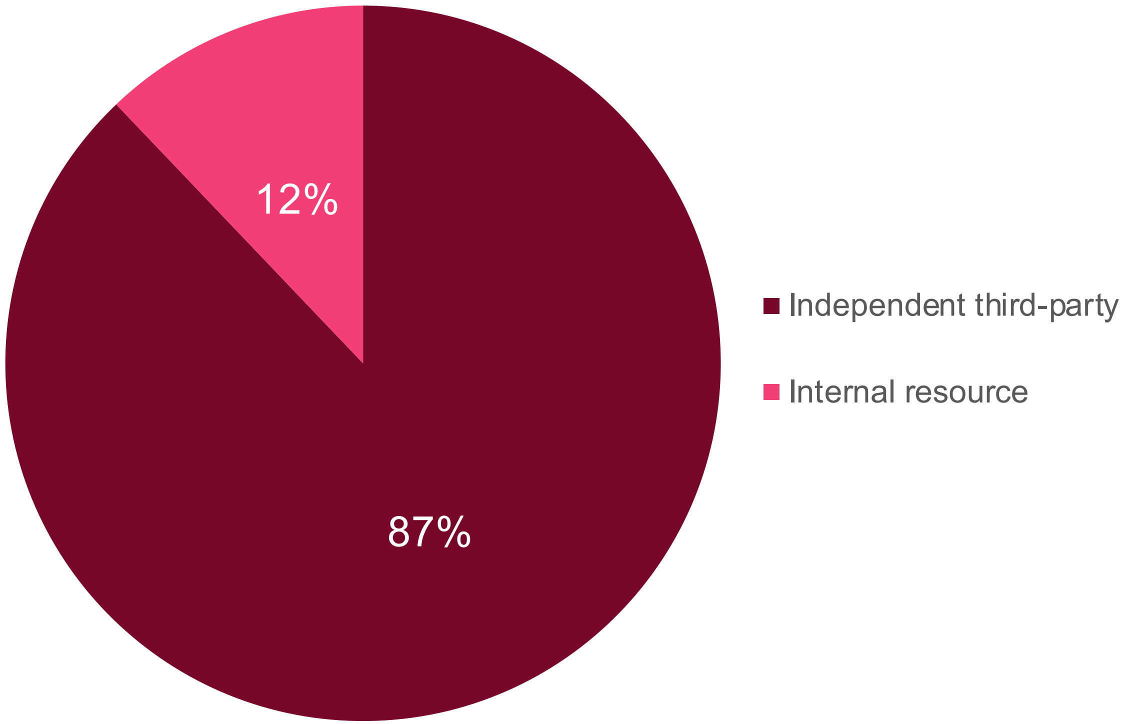
Completely in-house
5%

Q18. How often is your bank's staff required to participate in cybersecurity training? Q19. How has your bank executed staffcybersecurity training? Select all that apply. Q20. How frequently does your bank conduct incident response plan (IRP) tabletop exercises? (n=125)

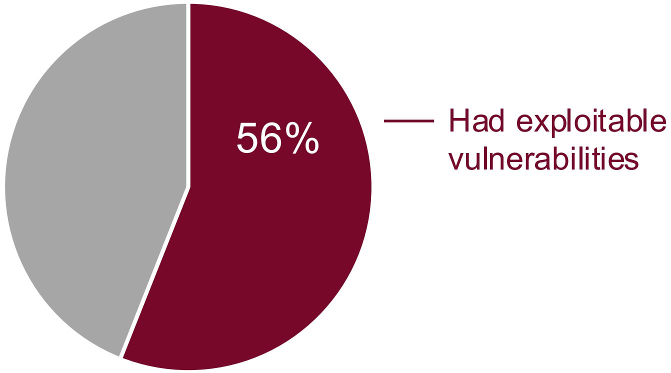
Penetration Tests

Most penetration tests are run by a third-party. 56% of respondents work at a bank that has had test results show exploitable vulnerabilities, all of which implemented measures to protect against those vulnerabilities.

Internal vs. External Penetration Tests



Penetration Test Results



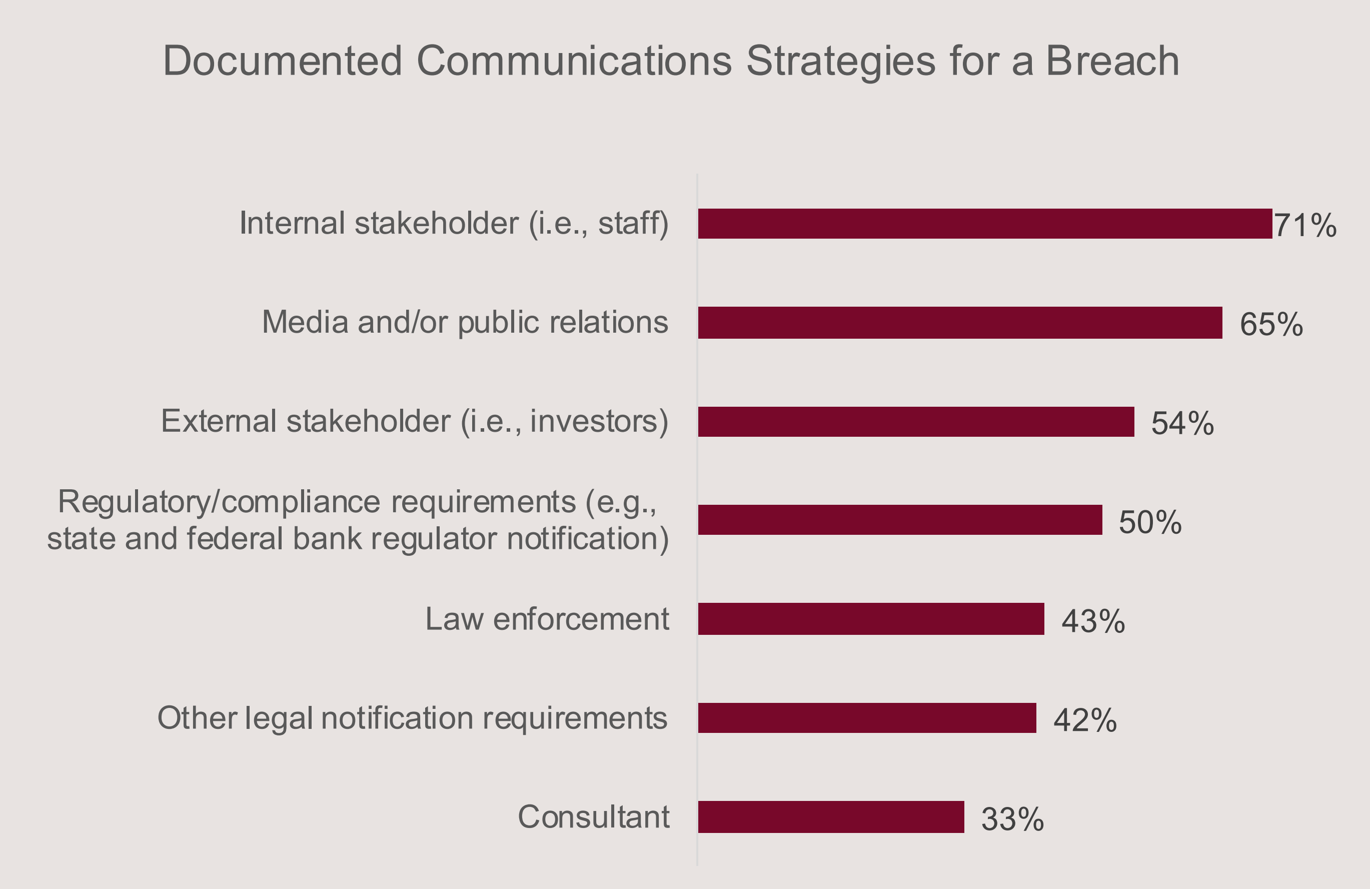
100%

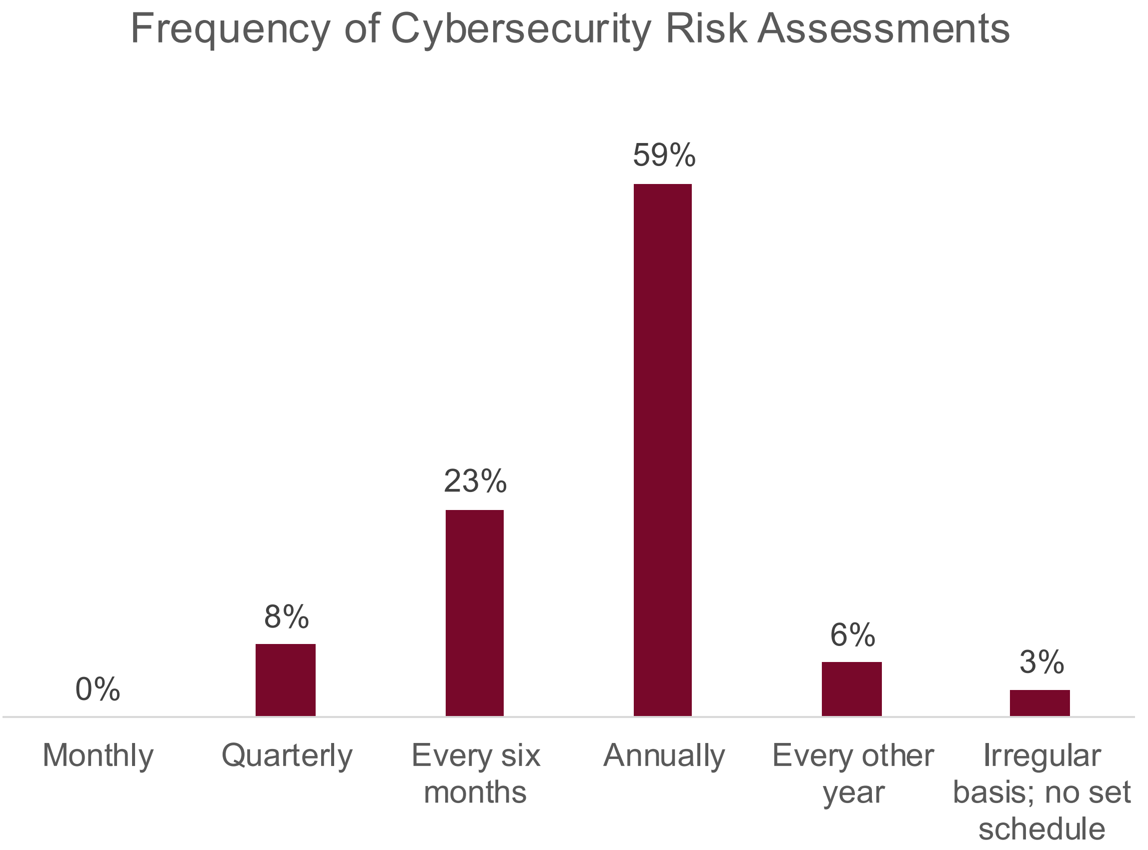
Implemented measures to protect against vulnerabilities revealed in the test

Q23. Was the last penetration test at your bank conducted by an internal resource or an independent third-party? (n=125) Q24. Did the penetration test reveal exploitable vulnerabilities? (n=124) Q25. Did your bank implement new or additional cybersecurity measures to protect against exploitable vulnerabilities revealed during that test? (n=69)

Breach Communication & Risk Assessments

Most commonly documented communication strategies in the event of a breach are internal stakeholders and media/PR. Cybersecurity risk assessments are most commonly done annually.



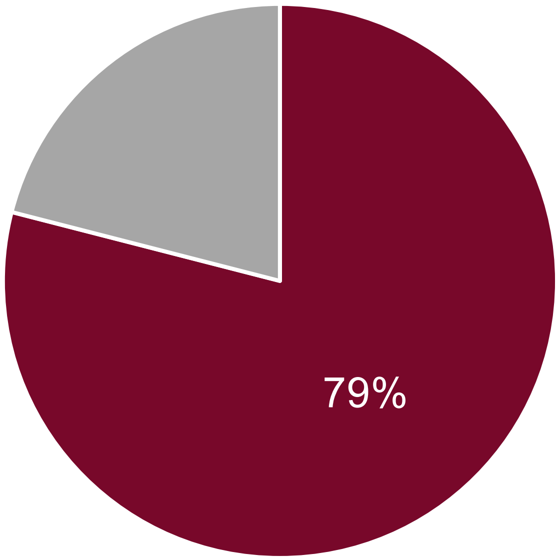


Q21. In the event of a major breach, for which of the following areas/groups do you have a documented communications strategy? Select all that apply. Q22. How frequently does your bank conduct cybersecurity-risk assessments? (n=125)

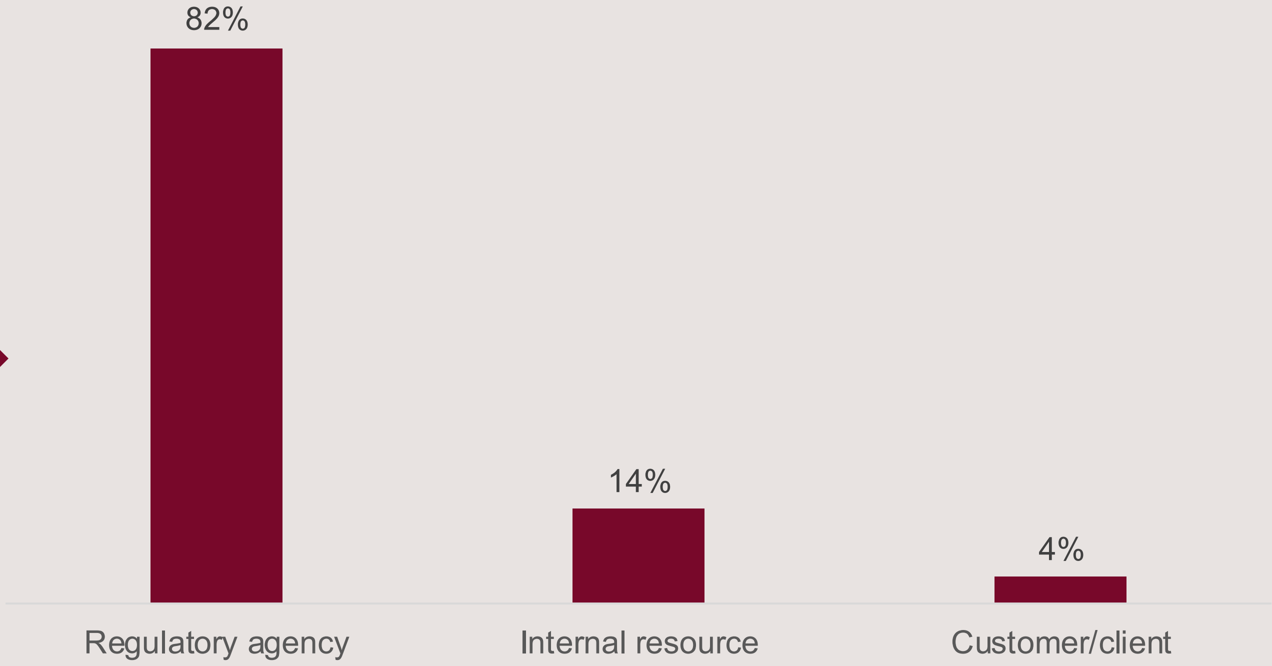
Breach Readiness Audit

Nearly 80% of conducted a breach readiness audit in the past year, most done by a regulatory agency.

Has Conducted Breach Readiness Audit in Past Year



Commissioner of Last Breach Readiness or Audit

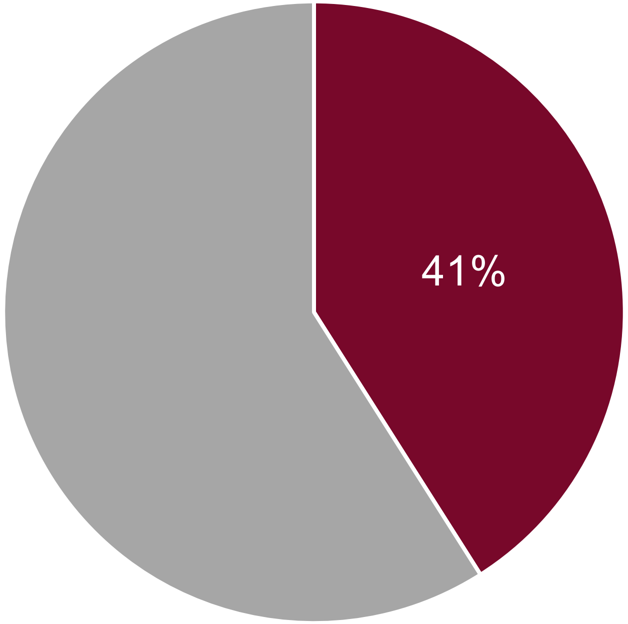


Q26. Within the past year, has your organization undergone a data security systems or breach readiness review or audit? (n=125) Q27. Who commissioned the last data security systems or breach readiness review or audit at your bank? (n=99)

Insurance Policy Review

Only 40% of banks have had their cyber-risk insurance policy reviewed to ensure it has sufficient coverage.

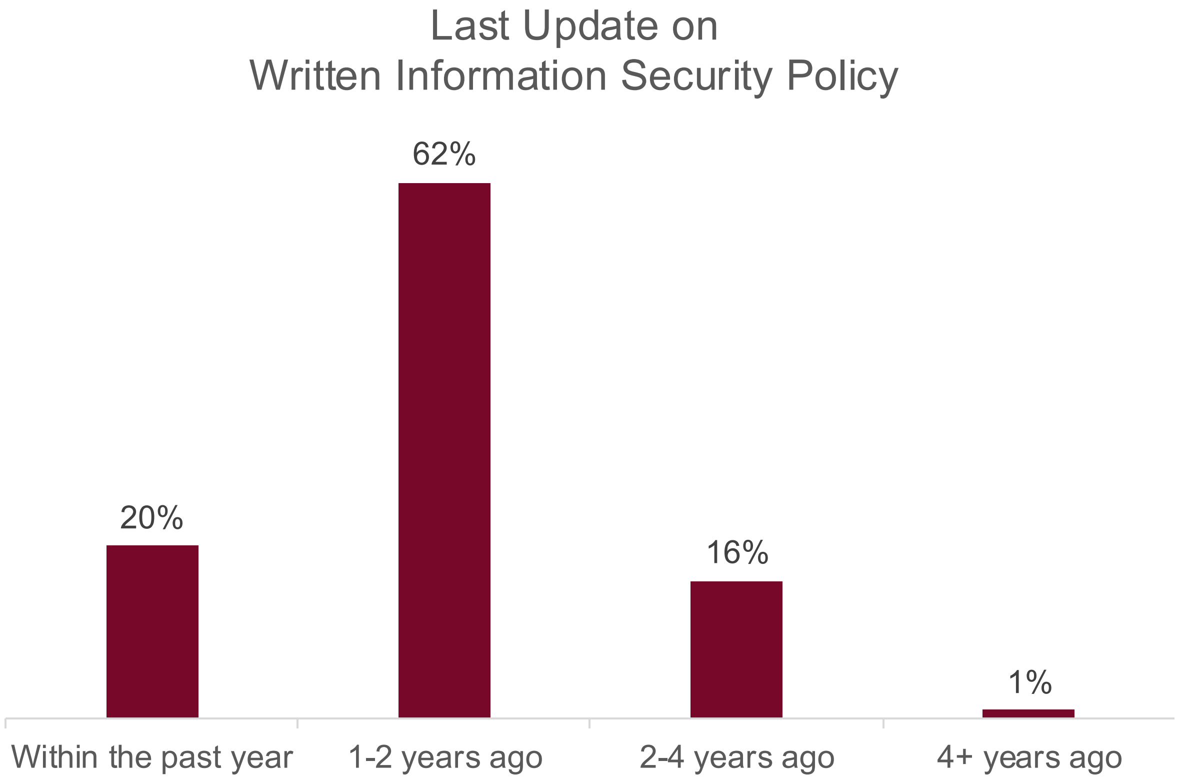
Cyber-risk Insurance Policy Reviewed for Adequacy of Coverage

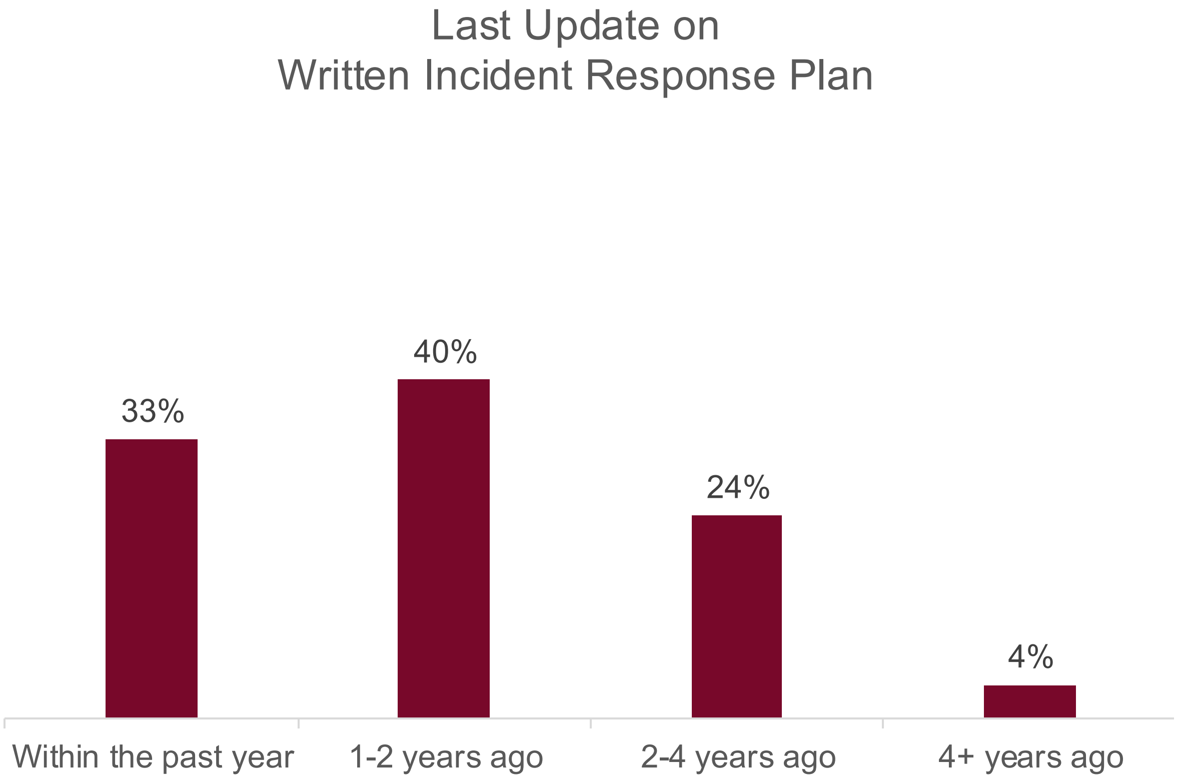


Q59. Have you had your cyber-risk insurance policy reviewed by counsel and/or other professionals to determine the adequacy of coverage? (n=125)

Updating Policies

The majority of banks have updated its written information security policy and written incident response plan within the past two years.

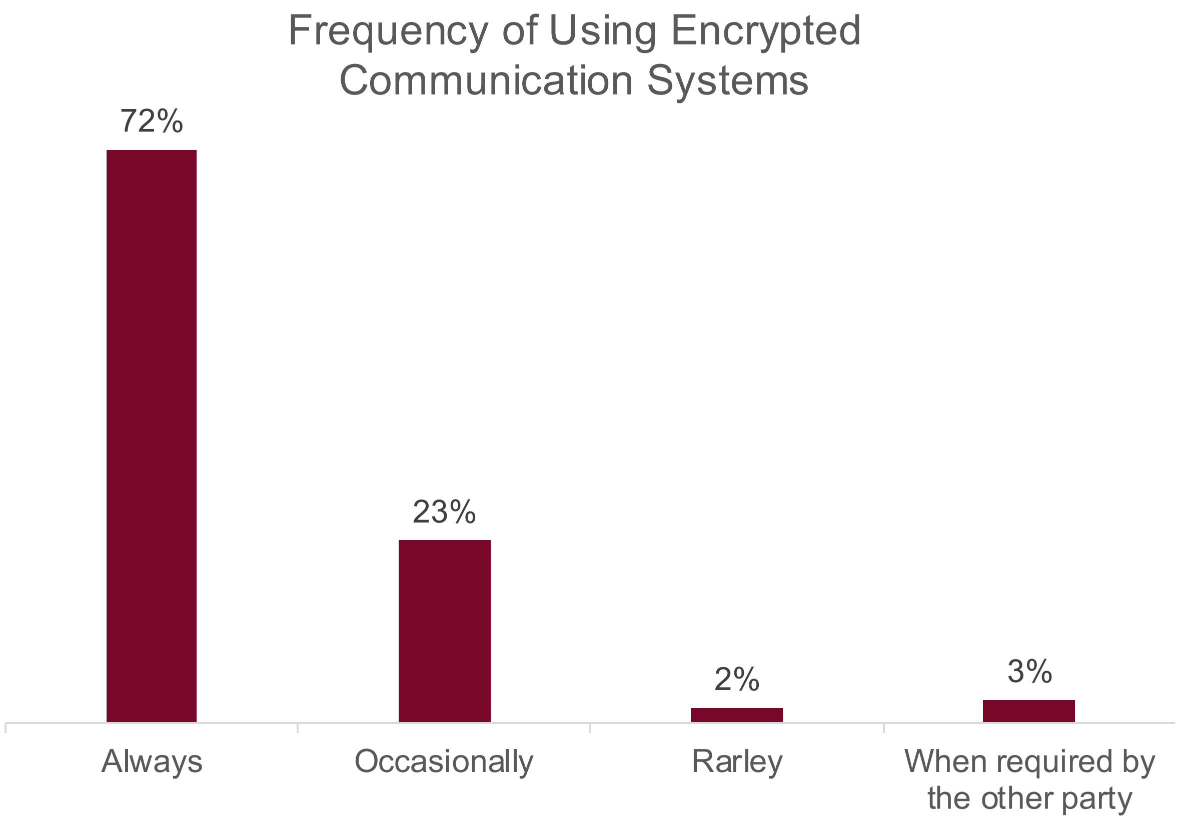


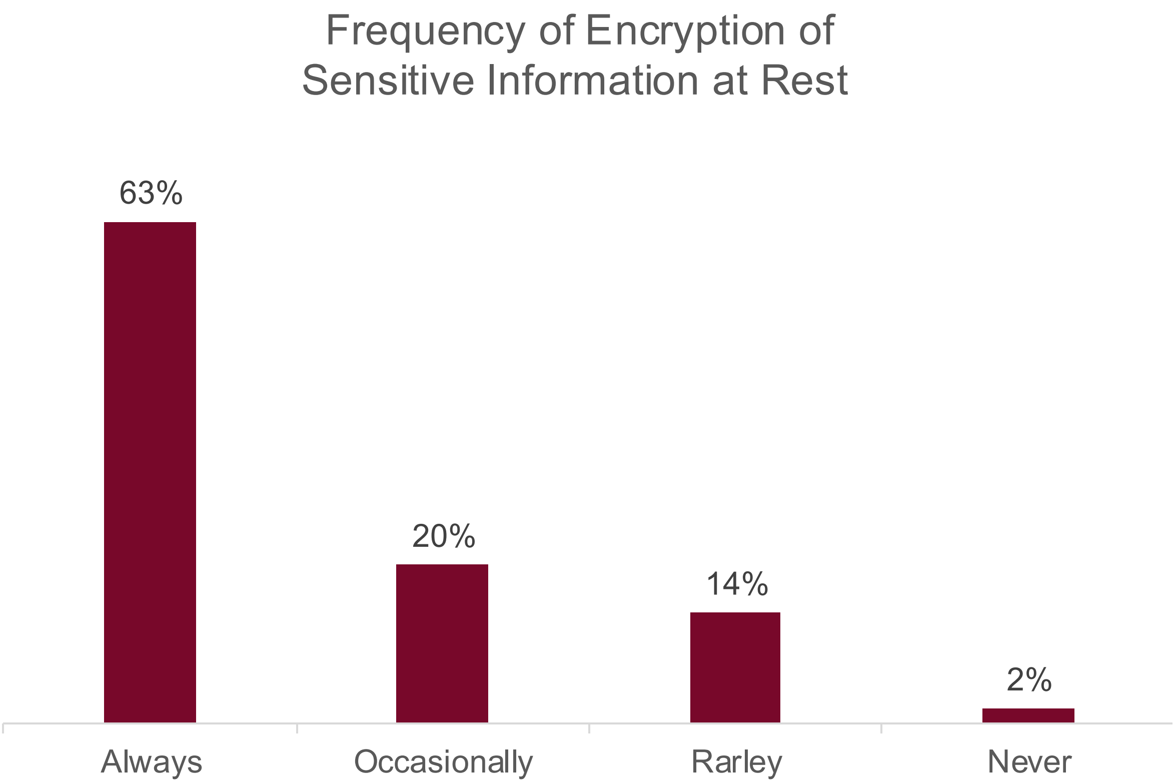


*Q55. How recently did your bank update its written information security policy? (n=125) Q56. How recently did your bank updat*e *its written incident response plan? (n=110)*

Encryption

Less than three-quarters of banks always use encrypted communication and even less always use encryption for sensitive information that is stored.



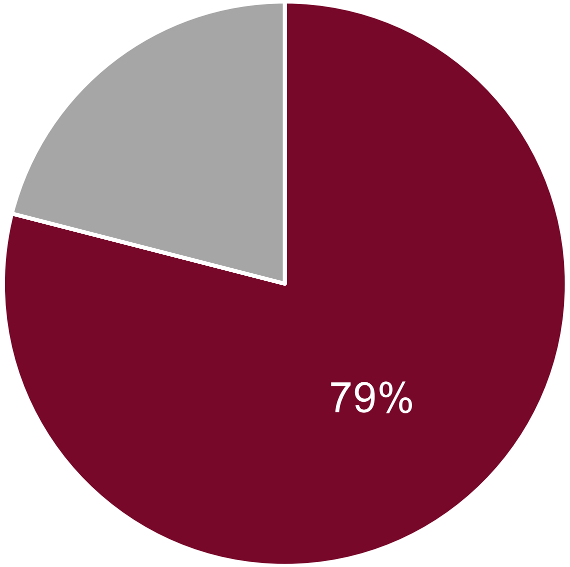


Q57. How often does your bank use encrypted communication systems to transmit sensitive information? Q58. How often does yourbank encrypt sensitive information that is at rest and/or stored? (n=125)

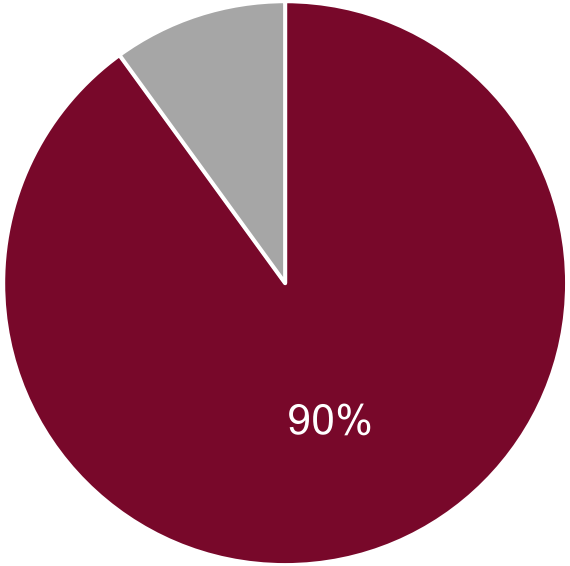
Collaboration

80% of banks collaborate with other banks and 90% collaborate with outside organizations to reduce cybersecurity risks.

Collaborate With Other Banks to Reduce Cybersecurity Risks



Collaborate With Other Organizations to Reduce Risks To Cybersecurity in the U.S.

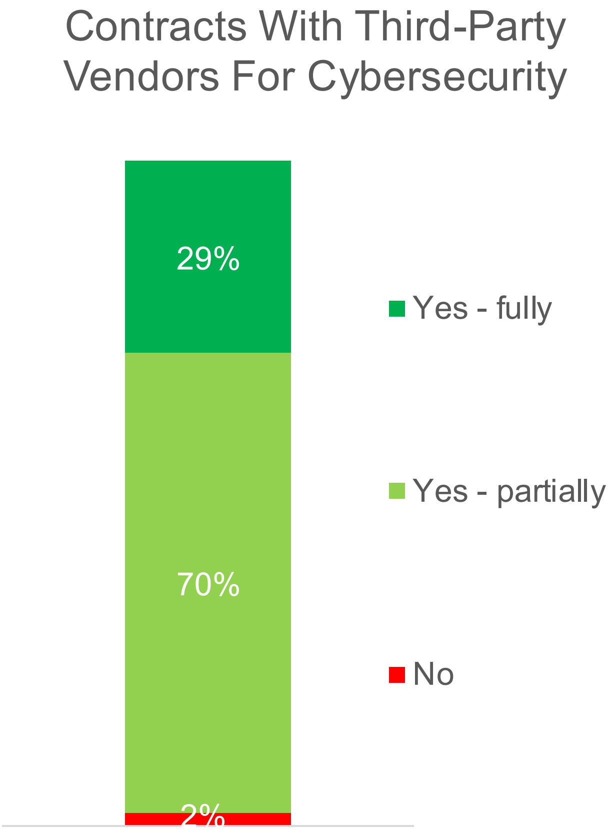


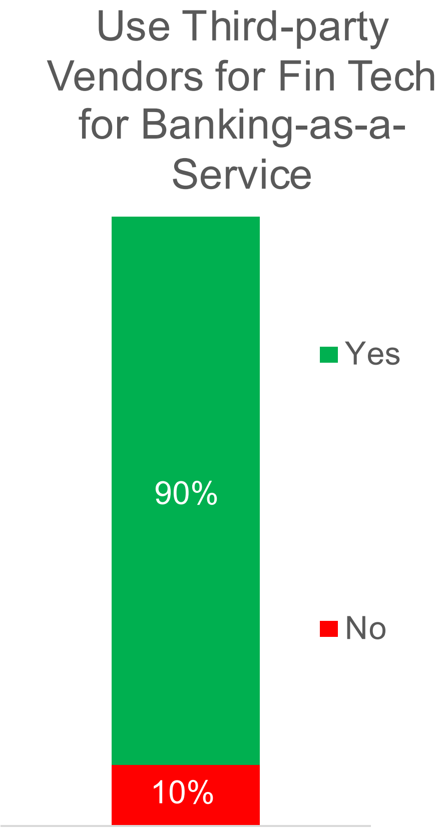
Q60. Does your bank formally collaborate with other banks to study ways to reduce risks to cybersecurity? Q61. Does your bankcollaborate with other organizations and agencies such as the American Bankers Association, various state banking associations, Independent Community Bankers Association, FF ISAC, etc., to study ways to reduce risks to cybersecurity in the U.S. and mid-size/regional banks? (n=125)

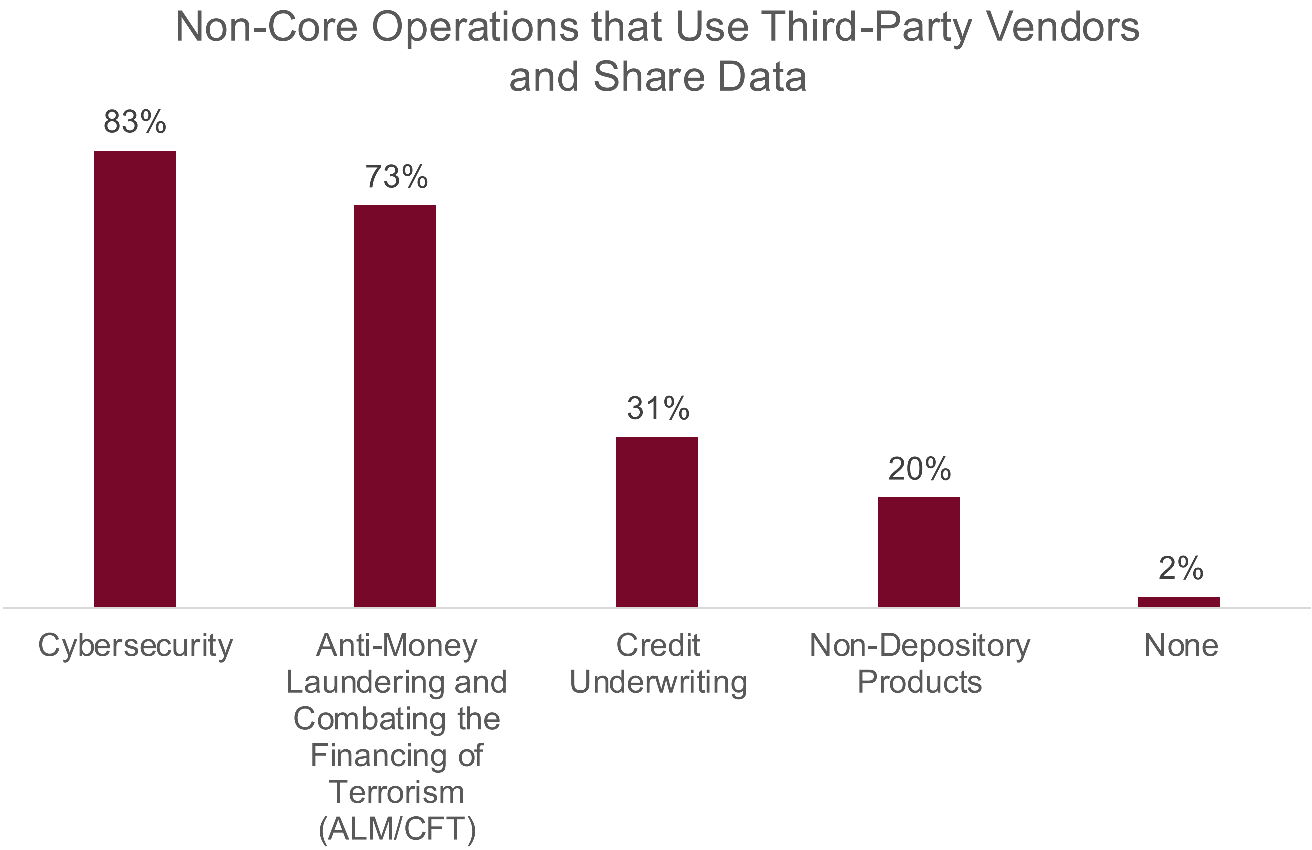
Third-Party Vendors

Third-Party Vendor Use

Most use third-party vendors for cybersecurity, fin-tech for banking-as-a-service, and anti-money laundering.







Q28. Does your bank contract with any third-party vendors for cybersecurity operations? Q29. Does your bank contract with any third-party vendors for Financial Technology (i.e., "FinTech") utilized to provide Banking-as-a-Service to customers? Q30. For what other non-core operations do you utilize third-party vendors and/or software and for which you share customer data? Select all that apply. (n=125)

Third-Party Vendor Due Diligence

While nearly all banks perform due diligence on third-party vendors, they are split on how they do so.

Review the third party's ability to comply with applicable laws and regulations	53%
Require third parties to supply cybersecurity policies and plans	51%
Investigate third-party cybersecurity measures, policies, procedures	50%
Investigate breach incident history	43%
Test third parties' cybersecurity systems	42%
Contractually obligate third parties to adhere to data-security protections	42%
Evaluation of information for third party's legally binding arrangements with subcontractors	41%
Review of service provider report from federal banking agency	38%
Include third-party risk in incident response plan (IRP)	36%
Evaluation of the qualifications and experience of a third party's principals and other key personnel	30%
Require third parties to carry cyber risk insurance	30%
Provide training to third parties	29%
Review of SOC 2 Report	29%
Review the third party's overall business strategy and goals	26%
Review the third party's financial condition	25%
Evaluation of the volume and types of subcontracted activities	23%
Review of the third party's employee on- and off-boarding procedures	22%
Completion of cybersecurity questionnaire	15%
We do not perform due diligence regarding sub-contractors' and service providers' security systems	1%

Q31. What due diligence do you conduct on new third-party vendors involved in high-risk or critical activites? Select all that apply. (n=125)

Third-Party Vendor Monitoring

The most common third-party vendor monitoring method is reviewing ongoing compliance with laws and contractual obligations.

Review ongoing compliance with laws, regulations, and contractual obligations	62%
Review third party's response to incidents	52%
Review audit reports	50%
Review third party's response to changing threats and vulnerabilities	49%
Review the volume, nature, and trends of customer inquiries and complaints	42%
Review overall effectiveness of the third-party relationship	41%
Review training provided to employees	35%
Review of the third party's reliance on, exposure to, and use of subcontractors	32%
Review changes to, or lapses in, the third party's insurance coverage	30%
Review changes to the third party's business strategy and its agreements with other entities	23%
Review changes in the third party's financial condition	23%
Review changes in the third party's key personnel	19%

Q32. Once a relationship is established with a new third-party vendor involved in high-risk or critical activities, what on-going monitoring do you preform? Select all that apply. (n=125)

Contract Requirements for Vendors in High-Risk Activities

The right to audit, prompt notification of a data breach, defined performance measures and complying with information security federal banking guidance are the top requirements for vendors involved in high-risk activities.

Require right to audit
58%

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

Defined performance measures
50%

Require vendor to maintain information security program that complies with federal banking guidance
50%

Specification of the type and frequency of reporting (performance, financial, security, etc.)
46%

Require performance be subject to regulatory oversight
41%

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

Require notification of significant strategic or operational changes, such as mergers, acquisitions, divestitures, subcontractors, key personnel changes, or other business initiatives
26%

Prohibit the use and disclosure of banking organization and customer information (except as necessary to provide contacted activities)
25%

Indication of ownership and license
25%

Indemnification requirement for data breach
23%

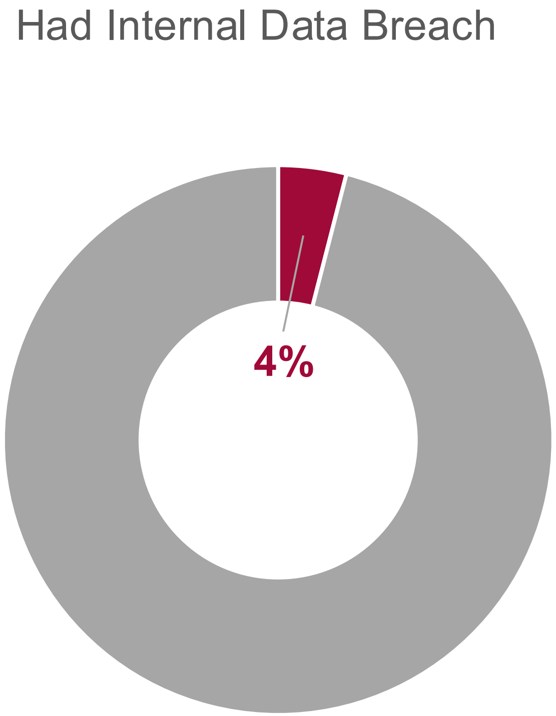
Insurance requirements
23%

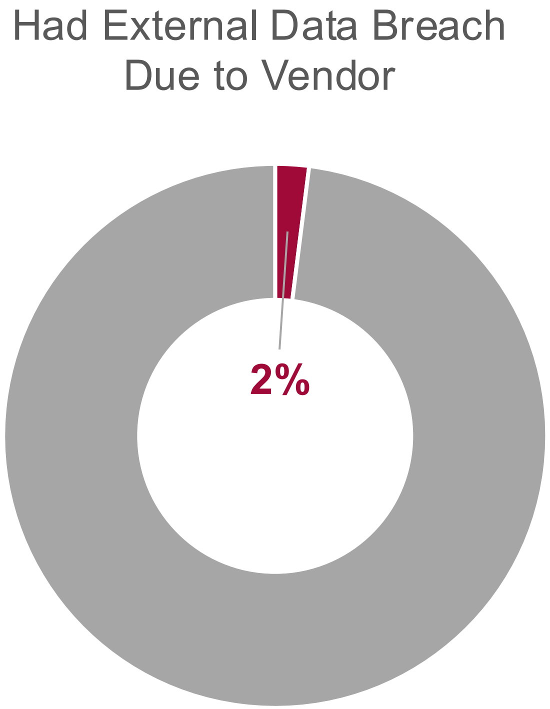
Q33. What contractual requirements do you impose on vendors involved in high-risk or critical activites, if any? Select all that apply. (n=125)

Breaches

Internal & External Breaches

Very few banks have had a breach, either internal or external.





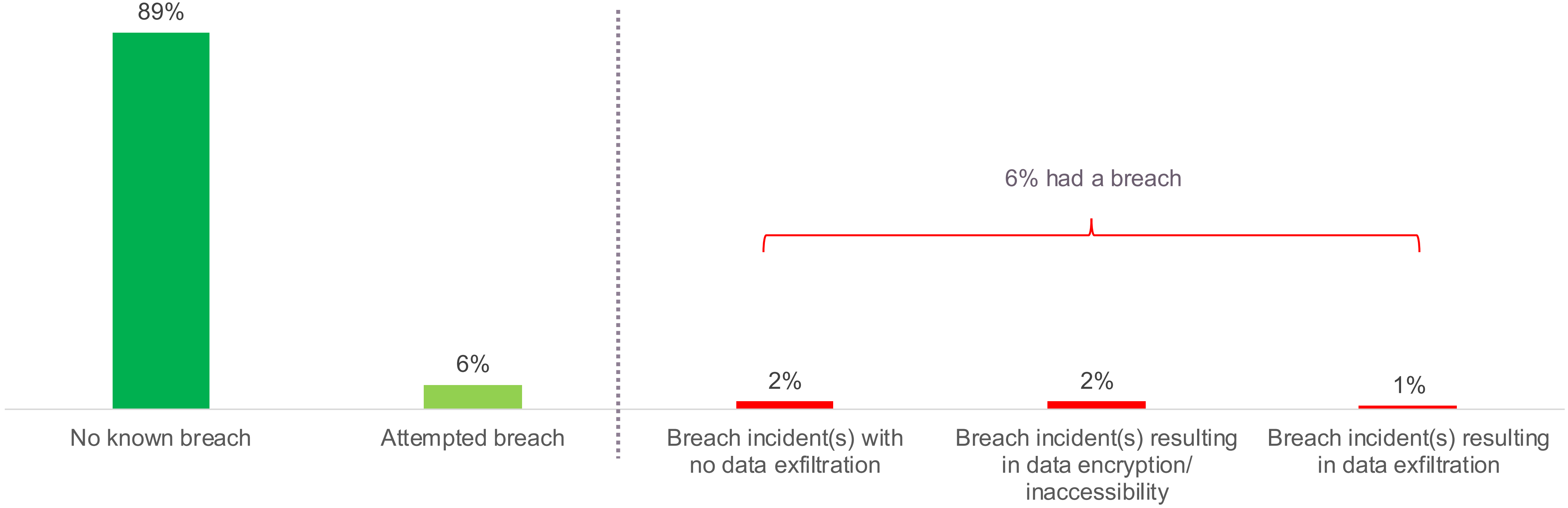
Among the small number of breaches, roughly half had <100 customers affected and half had 100-499 customers affected

Q35. Within the past three years, have you experienced an internal data breach affecting systems that the bank controls thatrequired notice to affected customers? (n=125) Q36. How many customers were affected by the internal data breach? (n=5) Q37. Within the past three years, have you had an external data breach attributed to a vendor that required you to givenotice to customers? (n=125) Q38. How many customers were affected by the external/vendor data breach? (n=2)

Data Breaches

The small number of banks that have had a breach are split on the type of breach.

Ways In Which Bank's Systems Have Been Compromised



Q34. Within the past three years, in what way(s) has your bank's systems and/or data been compromised? Select all that apply.(n=125)

Data Breach Details (7 respondents)

Nature of Attack	# of responses
Social engineering attacks (e.g., phishing, vishing, smishing)	4
Credential theft/account takeover	3
Malware infection	2
Ransomware	2
Business email compromise (BEC)	2
Third-party vendor attack	2
Misconfiguration or unpatched systems	1
Exploitation of software vulnerabilities	1

Malware and Ransomware Effects	# of responses
Encryption of data, rendering it inaccessible	2
Data corruption or destruction	2
Data exfiltration without encryption	1
Installation of backdoors or persistence mechanisms	1

Ransom Amount Paid	# of responses
$1,000-$50,000	1
$50,001-$100,000	1

Q40. What was the nature of the attack that resulted in the compromise of the bank's system? Select all that apply. (n=7) Q41 What were the malware and/or ransomware effects on the bank's systems? Select all that apply. (n=3) Q42. If your bank paid a ransom in response to a ransomware attack, what amount was paid? (n=2)

Data Breach Details (7 respondents)

Vulnerabilities Involved in Breach	# of responses
Insiders (current or former employees, contractors)	3
Third-party vendors	3
Web application vulnerabilities	3
Misconfigured network devices or firewalls	3
Weak or compromised credentials	3
Unpatched security vulnerabilities	2
API (Application Programming Interface) vulnerabilities	2
Social engineering / phishing	2
Mobile device vulnerabilities	1
Enterprise software vulnerabilities (e.g., ERP, CRM systems)	1
Operational Technology (OT) / Industrial Control Systems (ICS)	1

Lawsuits Filed Due to Data Breach	# of responses
Class action lawsuits related to data breach	3
Lawsuits filed by individuals alleging identity theft	2
Fines or penalties imposed by regulatory bodies	2
Criticism in Report of Examination relating to data breach	2
Lawsuits filed by business partners or clients	1
No legal or regulatory consequences to date	4

Post-Breach Activities	# of responses
Successfully implemented post-breach preventative measures	7
Engagement with law enforcement after breach	5
Data breach disclosed to the public	2
Negative media coverage about the breach	0
Minimal to some negative reaction due to the breach	6
Somewhat decreased level of deposits	3
Less than 10 lost customers (others not sure how many)	2

Insurance Coverage For Loss From Data Breach	# of responses
Yes	2
No – was requested but denied	2
No – was never requested	3

Estimated Costs Due to Data Breach	# of responses
Less than $25,000	3
$25,000-$100,000	3
$100,001-$200,000	1

Q44. What vulnerabilities were involved in the data breach? Select all that apply. Q45. For the cybersecurity breach(es) your bank experienced in the past three years, were post-breach preventative measures implemented and successful? Q43. Did you engage with law enforcement and banking regulators in an investigation of the data breach? Q46. Was the data breach disclosed outside the company other than to law enforcement and/or banking regulators? Q47. Was there negative media coverage about the data breach? Q48. Were there negative reactions from customers and/or business partners to the data breach? Q49. How has your bank's level of deposits been impacted since the data breach? Q50. Approximately how many customers have you received questions from relating to the data breach? Q51. Approximately how many customers did your bank lose as a result of the data breach? Q52. Are you aware of any lawsuits or regulatory action against your bank from the data breach? Select all that apply. Q53. Did your cyber-risk insurance policy provide coverage for any loss relating to the data breach? Q54. What was the estimated costs to your bank associated with the data breach? (n=7)

Thank you!