

2024 Community and Mid-Size Banks Cybersecurity Survey [Video]

Article By:

Andrew R. Lee

Robert L. Carothers

Jason M. Loring

Lara Sevener

Thomas E. Walker, Jr.

Jones Walker LLP is proud to announce the findings of our **2024 Community and Mid-Size Banks Cybersecurity Survey**, the fourth in our series of industry-focused cybersecurity studies. The comprehensive report highlights significant vulnerabilities and areas for improvement among community and mid-size banks in the United States.

Based on responses from 125 banking executives, including senior risk, technology, and information security leaders, the survey provides a detailed assessment of the current state of cybersecurity awareness, confidence, and preparedness in the banking sector.

The Jones Walker 2024 Community and Mid-Size Banks Cybersecurity Survey outlines four key findings and offers guidance on how US community and mid-size banks can evaluate and improve cyber readiness.

Jones Walker 2024 Community and Mid-Size Banks Cybersecurity Survey Key Findings

- 1. Post-Incident Regulatory Compliance is Slowly Improving, but Prevention and Preparedness are Lacking:** The banking sector is highly regulated, which makes data security, data privacy, and data breach compliance a top priority for banking executives. However, only 42% of respondents felt their own bank was very prepared for cyber threats, considering that only 61% of banks have established specific incident response teams with clearly assigned roles and responsibilities and 37% fail to encrypt sensitive information.

2. The Lack of Due Diligence Performed on Third Party Vendors is a Significant

Risk: While virtually all, 99%, of community and mid-size banks rely in part or in full on the services of third-party vendors to address their cybersecurity needs, only 71% hold them accountable for contractual, legal, or regulatory liability and a mere 23% require vendors to indemnify them against data breaches.

3. Banks Are Underutilizing Outside Counsel and Cybersecurity Professionals: Fifty-seven percent of respondents do not engage experienced cybersecurity attorneys, increasing their exposure to regulatory and legal risks. In addition, only 32% use outside pre- and post-incident forensic consultants, potentially hindering effective breach response and recovery. On top of all of that, 59% have not reviewed their cyber insurance policies to ensure adequate coverage.

4. Responsibly Embracing Emerging Technology Delivers Significant

Advantages: Community and mid-size banks are hesitant to implement emerging technologies like artificial intelligence (AI) for cybersecurity enhancements. With large banks adopting AI, this hesitancy may make community and mid-size banks more vulnerable targets if they don't keep pace.

[Download the Report](#)

© 2025 Jones Walker LLP

National Law Review, Volume XIV, Number 354

Source URL: <https://natlawreview.com/article/2024-community-and-mid-size-banks-cybersecurity-survey-video>