Hilco Global
Asset Smarter

SMARTER PERSPECTIVE: CYBERSECURITY

The Rising Pressure on Mid-Sized Banks: Defending Against Hackers and Regulators Alike

By Alexander Niejelow and James Wolf

October 2025 Regional banks are in many ways the lifeblood of the geographies they serve. The solutions they offer to individuals and small- to medium-sized businesses power community investment through entrepreneurship, home acquisition, and consumer financing. Regional banks in the U.S. hold $6 trillion in total assets, $3.5 trillion in loans, and employ over 500,000 Americans. The close-knit connection to community and ability to be quick and flexible with considerable capital are what make regional banks an indispensable resource for consumers, small businesses, and state and local governments. Housing significant overall liquidity and large quantities of sensitive personal data, regional banks are attractive targets for cyber criminals, especially as the largest organizations employ significant capital to harden their defenses. As regulators have homed in on these institutions with new cybersecurity requirements and are handing out significant penalties for noncompliance, regional banks face the dilemma of having to adapt to an increasingly threatening cyber landscape and complex regulatory environment, while continuing to innovate to effectively serve and retain their customers.

Banks have long been seen as a prized target for cyber criminals, yet in recent years, cybercriminals have shifted from focusing on large institutions to mid-sized ones, exploiting smaller cybersecurity budgets and more constrained defenses via ransomware, phishing, and supply chain attacks. In 2024, banks with between $1-5B in assets saw a 138% uptick in attacks, and banks with over $5B in assets saw a 44% increase. Smaller and mid-sized banks in particular rely on customer trust and are deeply embedded in local economies, making them more likely to adhere to ransomware demands in order to maintain relationships and their reputation in the community. Moreover, the financial data and payment rails managed by regional banks are just as valuable to a bad actor as the same assets at a trillion-dollar institution, and this combination of high-value assets with perceived weaker defenses relative to global financial institutions puts regional banks in the sweet spot of a threat actor's purview. Moreso, there tends to be vendor concentration at community and regional banks, and breaching one supplier can open many attack avenues for a criminal – the Office of the Comptroller of the Currency recently flagged regional banks' reliance on a small set of vendors as a systemic risk issue.

Earlier this year, the Federal Reserve explicitly mentioned smaller banking organizations as an area of concern in their Cybersecurity and Financial System Resilience Report, noting the need to "enhance cybersecurity supervision of community banking organizations." Furthermore, in a 2024 Annual Survey of Community Banks (those with less than $10B in assets), 96% of respondents named cybersecurity as an "extremely important" or "very important" risk. This

expressed concern comes on the heels of a handful of impactful breaches at mid-sized institutions. In June 2024, Evolve Bank & Trust in Arkansas was targeted by the LockBit ransomware group. Evolve refused to pay the ransom demand, and private data was leaked to the dark web as a result. Evolve is currently facing a class-action lawsuit. Supply chain incidents have been notable challenges as well, as evidenced by the May 2023 vulnerability in the MOVEit file transfer software in which dozens of banks were impacted, and the third-party vendor breach at KeyBank in Ohio, which was disclosed in February 2025.

There has also been a recent increase in regulatory pressure on the financial sector, along with stricter enforcement. Over the last three years, regulators have introduced new guidelines forcing regional banks to raise the bar on cyber governance, controls, and incident reporting. Amendments to NYDFS Part 500 that took effect this May mandated stronger board oversight, annual risk assessments, and new requirements around MFA (multifactor authentication), EDR (endpoint detection & response), and centralized logging. The SEC also issued new cyber disclosure rules in late 2023, requiring more detailed reporting and faster incident disclosures. In addition, inter-agency guidance from the Fed, OCC, and FDIC in July 2025 tightened third-party risk management, while CISA proposed stricter ransomware disclosure rules. Regulators are enforcing policies more aggressively as well: OCC and FDIC monthly releases show steady consent orders tied to cybersecurity, while NYDFS has issued over a dozen Part 500 orders since 2022, totaling $100m in fines. Regional banks have faced actions for weak third-party risk management, internal controls, fintech relationships, and risk reporting. Taken together, consistent enforcement actions and policy releases signal a continued emphasis on penalizing non-compliance.

Already spread thin, cyber and IT departments within regional banks are consumed with compliance and reporting efforts, redirecting resources that would otherwise be focused on proactive defense. Traditional critical proactive activities such as threat hunting, penetration testing, upgrading tech stacks, and developing strategic roadmaps may be deprioritized as cyber departments are pulled into compliance mode. This can also foster an innovation deficit for proactive cyber defense. New threats targeting regional banks, particularly around AI and supply chain attacks, mean banks should be focusing on initiatives such as cloud-security controls and AI threat-detection that will be critical in the future of cyber resilience; however, these are not as relevant to current compliance obligations. Regulatory checklists can also impact operations during an incident response period, as limited resources may be forced to choose between focusing on the rapid disclosures and actually detecting and containing the incident. Thus, regional banks face a paradox, where regulatory compliance meant to strengthen cyber resilience can actually divert valuable resources away from the defenses it is designed to encourage.

Financial institutions, particularly mid-sized banks, are increasingly reliant on a suite of tech partners to innovate and provide outstanding client service to customers who expect frictionless, mobile-first banking solutions. These tech partnerships are a strategic necessity but also a cybersecurity risk. Third-party vendors result in an expanded attack surface for adversaries to target, as evidenced by the aforementioned supply chain attacks. Furthermore, regulators have been clear that banks retain ultimate responsibility for vendor risks. This includes evidence of third-party risk management frameworks during audits and expedient disclosures even if a breach originates with a vendor, rather than the bank itself. To properly weigh the upside of innovation via tech partners against the downside of outsourced risk, leaders at regional banks must lead with strong third-party governance frameworks. While this predicament is difficult to navigate, it has also opened the opportunity for forward-thinking regional banks to differentiate themselves in the eyes of customers. The regional banks best prepared to take on these new challenges should implement the following measures to best prepare for this new reality:

1. **Enterprise-wide Governance:** Particularly at smaller institutions where executives have more direct oversight of all business units, strong cyber resilience starts at the top. Financial-sector regulators and shareholders are demanding stronger governance at the executive and board level. The average data breach cost in the financial sector in 2024 was $6.8m and penalties routinely exceed seven figures, indicating a fiduciary responsibility for cybersecurity to be treated as an enterprise risk, the same

way credit risk or liquidity risk is.

2. **Supply Chain Risk Analysis:** Particularly when it comes to working with third-party vendors, each partnership should have a strong lens towards secure cyber hygiene. Regional banks should assess the existing cyber posture and processes of their partners and have a clear allocation of security responsibilities in contracts. Moreso, cyber resilience should be seen as a differentiator when deciding between technical partners to integrate with.
3. **Incident Response Preparation:** Organizations of all sizes should operate under the assumption that there will be a breach at some point, particularly those in a sector as frequently targeted as regional banks. Having a clear incident response plan in place for different types of attacks (ransomware, DDoS, third-party) and conducting tabletop exercises that simulate those scenarios will not only limit the impact of attacks but also ease the reporting burden on the back end by clarifying roles and practicing escalation paths.
4. **Utilize Third-Party Advisors for Expertise:** Much in the same way banks rely on third parties for product innovation, advisors and vendors can also complement the cyber operations of the in-house team.These parties can assist in compliance and audit preparation, proactive defense strategy, incident response planning, and provide an objective view of where to prioritize efforts in strengthening cybersecurity posture, thus freeing up internal resources to focus on areas where they add most value.
5. **Communication of Cyber Risk Prioritization to Customers:** Given the information customers trust banks with, and the numerous options individuals and small businesses have in terms of banking partners, a prepared cybersecurity posture is top-of-mind and people decide where to hold their money and conduct business. Banks with strong cyber programs in place should market this to customers and use it as a means to differentiate themselves from the market and make customers feel comfortable giving more business. The ability to highlight compliance, partnerships, and certifications related to cyber will promote transparency and trust to clients.

Banks that are proactive around cybersecurity are able to save costs in the long-run and turn cyber maturity into a competitive advantage. First, regional banks should understand that increased investment and attention to cybersecurity is the new normal. While investments in cyber defense and compliance measures may seem costly, they pale in comparison to the direct financial impact of a fine or cyber breach, not to mention the downstream effects from a loss of customer trust, a reputation as a vulnerable entity, and potential litigation implications.

Sources:

American Bankers Association

Allure Security

Office of the Comptroller of the Currency

The Federal Reserve

Conference of State Bank Supervisors

Evolve

American Banker

JD Supra

JD Supra

U.S. Securities and Exchange Commission

GreenbergTraurig

Industrial Cyber

Office of the Comptroller of the Currency

Federal Deposit Insurance Corporation

New York State Department of Financial Services

The Federal Reserve

IBM

ALEXANDER NIEJELOW

EXECUTIVE DIRECTOR

GLOBAL CYBER ADVISORS

PROFESSIONAL SERVICES

Alexander can be reached directly at aniejelow@hilcoglobal.com or 917.952.8315.

JAMES WOLF

DIRECTOR

GLOBAL CYBER ADVISORS

PROFESSIONAL SERVICES

James can be reached directly at jwolf@hilcoglobal.com or 917.382.3182.