

Strengthening Cyber Resilience in US Banking

Threats, Breach Lessons, and Compliance Priorities for Financial Institutions





TABLE OF CONTENTS

Executive Summary 3

Introduction: Banks are a Prime Cyber Target 3

The Current Threat Landscape 4

Persistent Cybersecurity Gaps Impacting Banking Sector 6

Practical Cyber Resilience Framework for U.S. Banks 7

Cyber Resilience Roadmap for U.S. Banks (30/60/90-Day) 8

Strategic Recommendations 10

How Black Box Helps Banks Operationalize Cyber Resilience . . .11

Conclusion 12

Abbreviations & References 13

Appendix:. 14

Executive Summary

The **U.S. banking sector** is among the most targeted industries in the global cybersecurity landscape. Financial institutions of all sizes-ranging from global banking giants and global systemically important banks (G-SIBs) to regional banks, community lenders, and credit unions-face a continuous barrage of ransomware attacks, nation-state intrusions, third-party supply chain compromises, and increasingly sophisticated fraud schemes enabled by artificial intelligence.

This white paper provides a comprehensive analysis of the current cyber threat environment facing banks, the regulatory landscape governing institutional responses, persistent capability gaps that leave the sector exposed, and a forward-looking set of strategic recommendations designed to materially enhance resilience.



Introduction: Banks are a Prime Cyber Target

No sector of the economy is more systemically consequential-or more relentlessly targeted-than the banking and financial services sector, particularly banking. Banks serve as the central nervous system of commerce: they hold wealth, process trillions of dollars in daily transactions, extend credit, and maintain the infrastructure upon which individuals, businesses, and governments depend. This central role is precisely what makes them so attractive to adversaries whose motivations range from financial gain to geopolitical disruption.

The threat landscape has evolved dramatically over the past decade. While earlier cybercriminals primarily focused on stealing credentials and conducting account takeover fraud, today's adversaries deploy multi-stage attack chains that combine social engineering, zero-day exploits, ransomware-as-a-service, and insider threats. Nation-state actors-notably those affiliated with Russia, China, North Korea, and Iran-have demonstrated both the intent and capability to cause systemic disruption to critical financial infrastructure.

Average data breach costs in the financial sector reached \$6.08 million in 2025. Attack speeds have increased 100x over the past four years due to AI-enabled campaigns. Sixty-five percent of U.S. financial firms were hit by ransomware in 2024-the highest rate ever recorded. The U.S. Federal Reserve's July 2025 Cybersecurity and Financial System Resilience Report warns of growing threats from nation-state actors, ransomware groups, and AI-enabled attacks, and highlights the risks associated with third-party providers.

The banking sector's own digital transformation has significantly expanded its attack surface. Cloud migration, real-time payment systems, open banking APIs (supporting the rapidly growing fintech industry), embedded finance partnerships, and mobile-first customer engagement have introduced new integration points and dependencies.

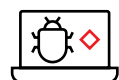
The Current Threat Landscape



Ransomware and Extortion

Ransomware has become one of the most disruptive and costly cyber threats facing financial institutions. In a typical attack, adversaries gain initial access through phishing, credential stuffing, or the exploitation of unpatched vulnerabilities; move laterally across the network; exfiltrate sensitive data; and then encrypt systems while threatening to publish the stolen data if a ransom is not paid—a tactic known as double extortion.

The financial services sector is particularly vulnerable because operational downtime carries immediate and measurable consequences. An inability to process transactions, access customer data, or maintain ATM networks results in significant regulatory, reputational, and customer impact. Service disruptions caused by cyber threats can also erode customer trust and drive customers away from affected institutions.



Advanced Persistent Threats

Advanced Persistent Threat (APT) groups sponsored by nation-states represent the most sophisticated adversaries facing U.S. financial institutions. These actors conduct long-dwell intrusions—often remaining undetected within networks for months—to carry out espionage, pre-position for potential disruptive operations, or enable large-scale theft. North Korea's Lazarus Group, for example, has stolen an estimated \$3 billion in cryptocurrency from financial institutions and exchanges since 2017 to fund the regime's weapons programs.

The potential for APTs to be used not only for theft but also for infrastructure disruption is an increasing concern for national security and financial stability authorities.





Business Email Compromise and Social Engineering

Business Email Compromise (BEC), in which adversaries impersonate executives, vendors, or counterparties to redirect wire transfers or obtain sensitive information such as credentials, cost U.S. organizations an estimated \$2.9 billion, according to FBI Internet Crime Complaint Center data. Banks are both victims and unwitting facilitators of BEC fraud, often processing misdirected transfers before the fraud is detected.

The emergence of AI-powered voice cloning and deepfake video technologies has significantly intensified social engineering attacks. Fraudsters can now convincingly impersonate individuals using synthetic audio or video, undermining authentication methods that rely on voice recognition or video verification.



Cloud, API, and Web Application Exposure

As banks modernize, they create new opportunities for innovation and new avenues for attack. Cloud platforms, web applications, and publicly exposed APIs increase agility but also require stronger configuration discipline, clearer ownership, and continuous visibility. Modernization without sufficient maturity can expand risk faster than institutions anticipate, increasing and extending the overall attack surface.



Third-Party and Supply Chain Risk

The most significant source of material cyber incidents in banking is not direct attacks on institutions, but compromises of third-party vendors, technology providers, and service partners. Banks rely on hundreds to thousands of third parties for functions ranging from core banking platforms and payment processing to cloud hosting, HR systems, and fraud analytics.

When a vendor is breached, every dependent institution is exposed. The 2020 SolarWinds supply chain compromise-in which malicious code was inserted into widely used network monitoring software-impacted multiple financial regulators and institutions. MOVEit, Accellion, and other file transfer platforms have been exploited in similar ways, exposing sensitive customer data across dozens of banks simultaneously.

These threats extend beyond security platforms. They can disrupt services, erode customer trust, increase legal and remediation costs, and trigger regulatory action. Cyber threats are now significant business risks that demand sustained leadership attention.



Persistent Cybersecurity Gaps Impacting Banking Sector



Third-Party Risk Management

Despite years of regulatory focus, third-party cyber risk management remains the most pervasive and consequential gap for banks. The challenge is both structural and practical. Structurally, banks depend on technology vendors—including a small number of highly concentrated providers for core banking, payment processing, and cloud infrastructure—that are not subject to the same regulatory requirements. Most banks operate within a vast vendor ecosystem, making meaningful security due diligence difficult.

Addressing this requires tiered vendor risk programs, continuous monitoring of third- and fourth-party dependencies and embedding cybersecurity standards and incident notification requirements into contracts from the outset. However, most banks still rely on periodic, questionnaire-based assessments.



Cyber Workforce Shortages

The global cybersecurity workforce gap exceeded 5 million unfilled positions in 2025, including a shortage of 500,000 in the U.S. alone, with banks competing against the technology, defense, and healthcare sectors for a limited talent pool. Within banks, the most acute shortages are in cloud security engineering, threat intelligence analysis, and incident response, with the impact particularly severe at community and regional institutions.

Addressing this gap requires a combination of strategies: developing internal talent through structured career pathways and rotational programs, partnering with universities and community colleges on curriculum development, expanding the use of managed security service providers, and investing in automation to reduce analyst workloads for routine tasks.



Legacy Technology Infrastructure

In the U.S., a substantial portion of bank infrastructure still relies on legacy technologies, with COBOL-based mainframe systems remaining widespread. These systems are difficult to patch, monitor with modern security tools, and integrate with contemporary zero-trust architectures. Modernizing them is disruptive, costly, operationally risky, and organizationally complex, leading many institutions to defer transformation while accumulating technical debt.

This legacy infrastructure also limits the ability to implement modern security controls such as micro-segmentation, real-time monitoring, continuous authentication, and behavioral analytics—capabilities critical for detecting today's threats.



Board and Executive Cyber Governance

Effective cyber resilience requires governance structures that elevate cyber risk to the same level of board attention as credit, market, and liquidity risks, as all have the potential to disrupt business operations. While progress has been made, and many large institutions now have board-level cybersecurity oversight, the depth and quality of that oversight vary significantly.



Practical Cyber Resilience Framework for U.S. Banks



Lead with Risk-Based Cybersecurity

Banks should prioritize controls based on business criticality, customer impact, and operational dependencies. A risk-based model enables leadership to focus on what matters most rather than pursuing uniform maturity across all domains.



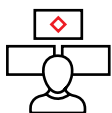
Strengthen Governance and Executive Oversight

Cybersecurity requires clear ownership, board visibility, and consistent reporting. Governance is more effective when cyber discussions are aligned with resilience, business continuity, and risk acceptance rather than limited to technical detail.



Focus on Identity, Access, and Privileged Control

In modern banking environments, identity is central to both defense and disruption. Strong authentication, least-privilege access, privileged access monitoring, and disciplined third-party access management should be treated as core resilience capabilities.



Improve Monitoring, Evidence, and Response Readiness

Banks need centralized visibility, reliable control evidence, and well-tested incident response processes. Response readiness is no longer limited to emergency action—it requires demonstrating operational control under stress.



Integrate Third-Party Risk into the Cybersecurity Core

Third-party cyber risk should not remain peripheral to the program. It must be integrated into access governance, monitoring, incident planning, and executive reporting, as external dependencies are now too significant to manage otherwise.





Cyber Resilience Roadmap for U.S. Banks (30/60/90-Day)

For many banks, the challenge is not recognizing the need for stronger cybersecurity but translating priorities into a focused execution plan that enhances resilience without creating unnecessary operational burden. A 30/60/90-day roadmap enables leadership teams to sequence actions in a visible, risk-based manner aligned with both regulatory expectations and operational realities

First 30 Days: Establish Visibility, Ownership, and Risk Priorities

- Identify the most critical business services, supporting systems, privileged access paths, and third-party dependencies.
- Validate current cyber governance, including executive ownership, escalation paths, and decision authority.
- Assess readiness across key risk areas: identity and access management, monitoring coverage, incident response, and third-party exposure.
- Confirm the bank's ability to quickly determine whether an incident meets regulatory notification or supervisory thresholds.
- Review logging, alerting, and telemetry coverage across high-value environments, including core banking, cloud, identity, and customer-facing systems.
- Prioritize the highest-impact control gaps based on business criticality, operational exposure, and regulatory relevance.

Next 60 Days: Tighten Controls and Improve Operating Discipline

- Strengthen identity controls through least-privilege access, privileged account reviews, multi-factor authentication enforcement, and tighter third-party access governance.
- Enhance monitoring and detection coverage across critical systems, identities, and external-facing assets to reduce blind spots and investigation delays.
- Streamline workflows across security, risk, compliance, infrastructure, and vendor management teams to address ownership gaps.
- Standardize evidence collection for key cybersecurity controls so incident response, compliance, and audit functions rely on consistent data.
- Review and strengthen third-party cyber risk processes, including onboarding diligence, access restrictions, monitoring expectations, and contractual accountability.
- Establish focused executive reporting that tracks core resilience indicators such as exposure, response readiness, control effectiveness, and operational risk.

By 90 Days: Validate Readiness and Operationalize Resilience

- Conduct targeted tabletop exercises for high-impact scenarios such as ransomware, identity compromise, third-party disruption, and cloud control failures.
- Validate that incident escalation, regulatory notification, communication flows, and decision authority function effectively under realistic conditions.
- Confirm that strengthened controls produce reliable operational evidence to support both management reporting and supervisory review.
- Measure whether improvements in monitoring, access governance, and response reduce operational friction and improve time to detect and contain incidents.
- Embed cyber resilience reviews into a recurring governance cadence involving security, risk, compliance, technology, and executive leadership.
- Transition from one-time remediation to a continuous improvement model that leverages lessons learned, metrics, and threat trends to refine the cybersecurity operating model over time.

This roadmap is not intended to complete a full transformation within one quarter. Its purpose is to establish early control clarity, strengthen operational discipline, and create a repeatable resilience model that leadership can govern with confidence.





Strategic Recommendations

Based on this analysis, the following strategic recommendations are offered for banking institutions, industry associations, and regulators:

Priority	Recommendation	Timeframe
Critical	Implement continuous, risk-tiered third-party cyber monitoring replacing periodic questionnaire assessments	4 months
Critical	Establish or strengthen board-level cyber governance with at least one director possessing substantive cyber expertise	4 months
Critical	Align incident detection and response capabilities to achieve sub-72-hour detection for high-severity incidents	6 months
High	Develop and test a cloud concentration risk scenario - including exit strategies for critical cloud-dependent workloads	6 months
High	Launch AI-enabled threat detection capabilities in the Security Operations Center, prioritizing behavioral analytics	12 months
High	Conduct cryptographic inventory assessment and develop a post-quantum migration roadmap	12 months
High	Establish or deepen engagement with FS-ISAC for threat intelligence sharing and sector-wide exercise participation	Ongoing
Moderate	Invest in cyber workforce pipeline through university partnerships, apprenticeships, and internal rotational programs	24 months
Moderate	Advocate through industry associations for harmonized federal cyber incident reporting standards	24 months
Moderate	Integrate cyber resilience metrics into executive and business-line performance management frameworks	24 months

How Black Box Helps Banks Operationalize Cyber Resilience

✓ **Translating Cyber Resilience into Operational Reality**

Black Box helps banks move beyond cybersecurity strategy as a planning exercise and transform resilience into a live operating capability that protects critical services, supports business continuity, and withstands regulatory scrutiny.

✓ **Designing Security for the Modern Banking Risk Environment**

As banking risk spans identities, cloud environments, digital channels, core platforms, and third-party ecosystems, Black Box helps institutions replace fragmented controls with a coordinated cybersecurity model aligned to today's threat and operating landscape.

✓ **Aligning Security Investment to What Matters Most**

We help banks prioritize cybersecurity around business-critical services, high-value assets, privileged access paths, operational dependencies, and concentration risks, ensuring resilience efforts are directly tied to measurable business and regulatory outcomes.

✓ **Strengthening the Foundational Controls that Define Resilience**

Black Box delivers deep cybersecurity capabilities across identity and access management, privileged access management, Zero Trust architecture, cloud and infrastructure security, vulnerability and exposure management, governance alignment, and security program modernization.

✓ **Modernizing Security Operations for Speed, Visibility, and Control**

We help institutions enhance telemetry, centralize monitoring, strengthen SIEM- and XDR-aligned operations, improve detection engineering, and elevate incident response readiness, enabling security teams to identify, investigate, and contain threats with greater precision.

✓ **Connecting Technical Controls to Executive and Regulatory Confidence**

Our approach strengthens both controls and control evidence. By aligning monitoring, escalation workflows, response playbooks, and reporting structures, Black Box enables banks to demonstrate that resilience is actively governed and operationally validated.

✓ **Integrating Third-Party Risk into the Core Security Program**

Recognizing the growing impact of vendor, platform, and service provider exposure, Black Box helps banks integrate third-party risk into access governance, monitoring, incident preparedness, and accountability frameworks rather than treating it as a standalone compliance activity.

✓ **Delivering a More Defensible and Sustainable Cybersecurity Posture**

By combining advisory, architecture, integration, and managed security services, Black Box enables banks to shift from reactive remediation to continuous resilience improvement, creating a cybersecurity posture that is technically stronger, operationally clearer, and more defensible to leadership, auditors, and regulators.

Conclusion

Cyber resilience in U.S. banks is not a one-time effort; it is a continuous organizational capability that must evolve as quickly as the threats it faces-if not faster. The good news is that foundational elements are largely in place: regulatory frameworks, industry associations, threat intelligence-sharing mechanisms, and a growing base of institutional expertise. The challenge lies in execution-ensuring these frameworks translate into operational capability, governance structures drive accountability and expertise, and resources are focused on areas of greatest systemic risk.

Banks that succeed in the next decade will treat cyber resilience not as a compliance obligation, but as a strategic capability. It must be managed as a core business initiative-owned by the board and/or CEO, integrated across business and technology functions, and continuously tested and refined. While the CISO and security organization may own day-to-day operations, overall strategy must be driven at the board level.

The cost of failing to build this capability is not merely financial. A major, sustained cyberattack on a U.S. bank could not only cripple the institution but also erode public confidence, disrupt access to credit and payment services, and create cascading effects across the broader economy.

Final Thought

The question facing every banking institution is not whether a material cyber incident will occur, but whether the organization has built enough resilience to detect it early, contain it rapidly, and recover completely - without compromising customer trust or systemic stability. That answer must be yes.



Abbreviations

- AI** - Artificial Intelligence
- API** - Application Programming Interface
- FFIEC** - Federal Financial Institutions Examination Council
- FTC** - Federal Trade Commission
- GLBA** - Gramm-Leach-Bliley Act
- IAM** - Identity and Access Management
- MFA** - Multi-Factor Authentication
- NYDFS** - New York State Department of Financial Services
- PII** - Personally Identifiable Information
- SEC** - U.S. Securities and Exchange Commission
- SOC** - Security Operations Center

References

1. *NIST Cybersecurity Framework 2.0*
2. *FFIEC IT Examination Handbook: Information Security Booklet*
3. *Interagency Guidelines Establishing Information Security Standards*
4. *FFIEC Authentication and Access to Financial Institution Services and Systems*
5. *Computer-Security Incident Notification Final Rule*
6. *NYDFS 23 NYCRR 500: Cybersecurity Requirements for Financial Services Companies*
7. *SEC Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure*
8. *Capital One Announces Data Security Incident*
9. *SEC Order: ICBC Financial Services LLC*
10. *Verizon 2025 Data Breach Investigations Report: Finance Snapshot*



Appendix:

A1. The Regulatory Framework: Progress and Fragmentation

The U.S. banking sector operates within a layered, multi-agency regulatory regime that has produced a growing body of cyber-specific guidance and requirements. While recent years have seen meaningful convergence, the framework remains fragmented in ways that create compliance burdens and leave residual coverage gaps.

✓ **NIST Cybersecurity Framework (CSF)**

The NIST CSF—originally published in 2014 and significantly updated to version 2.0 in 2024—provides the foundational, risk-based structure most U.S. financial institutions use to organize their cybersecurity programs. CSF 2.0 introduces a new Govern function, elevating cybersecurity governance to the same level as Identify, Protect, Detect, Respond, and Recover. While voluntary for most institutions, alignment with the CSF is effectively expected by major banking regulators as a baseline.

✓ **FFIEC Cybersecurity Assessment Tool and Guidance**

The Federal Financial Institutions Examination Council (FFIEC) has issued a comprehensive set of cybersecurity guidance applicable across major banking regulators (OCC, FDIC, Federal Reserve, NCUA, CFPB). The FFIEC Cybersecurity Assessment Tool (CAT) maps institutional risk profiles to maturity levels across five domains. Ongoing updates reflect evolving threats, including guidance on cloud security, authentication, and vendor risk management.

✓ **OCC Guidelines on Operational Risk and Heightened Standards**

The Office of the Comptroller of the Currency integrates cybersecurity into its operational risk framework for large and complex institutions. Under Heightened Standards (12 CFR Part 30, Appendix E), covered banks must maintain robust risk governance frameworks, including cyber risk, with clearly defined board-level accountability.

✓ **SEC Cybersecurity Disclosure Rules (2023)**

The SEC's 2023 cybersecurity rules—applicable to publicly traded financial institutions—require disclosure of material incidents within four business days of determining materiality, along with annual disclosures of cybersecurity risk management processes and board oversight. These requirements have elevated cyber risk within investor relations and corporate governance discussions.

✓ **DORA (EU) and Cross-Border Implications**

While not a U.S. regulation, the EU's Digital Operational Resilience Act (DORA), effective January 2025, has significant implications for U.S. banks with European operations. DORA imposes prescriptive requirements for ICT risk management, incident reporting, operational resilience testing, and third-party oversight. U.S. institutions with EU exposure must align their programs across both regulatory frameworks.

A2. Major U.S. Banking Breaches

1. One of the largest U.S. banks reported a 2014 breach affecting 7 million small businesses and 76 million households. Attackers gained access through a compromised employee account. While no financial data was stolen, hackers obtained names, phone numbers, email addresses, physical addresses, and a list of applications used by the bank, potentially enabling future exploits.
2. In 2017, a global data, analytics, and technology company failed to patch a well-known Apache Struts vulnerability for months, resulting in a catastrophic breach affecting nearly 148 million individuals. The incident remains one of the most significant breaches in U.S. financial history.
3. In 2008, a major financial technology company experienced a cyberattack in which attackers injected malware through a web form, compromising approximately 130 million credit and debit card numbers via SQL injection. The attackers remained undetected for nearly six months, installing sniffer software to capture payment card data in transit.
4. In 2024, another century-old financial institution experienced a data breach involving customer names, Social Security numbers, account numbers, dates of birth, and contact information. The incident occurred in May and was disclosed in late June. The bank's fintech partnerships amplified the impact, and the attack was attributed to the LockBit ransomware group.
5. A U.S. regional bank experienced multiple breaches through MOVEit Transfer and Accellion FTA vulnerabilities, illustrating the consequences of delayed patching.
6. In 2025, a cyberattack exploited a known but unpatched firewall vulnerability at a financial technology service provider, leading to unauthorized access across dozens of banks and credit unions. The breach affected at least 400,000 individuals nationwide, with most impacted residents in Texas. Compromised data included Social Security numbers and bank account details. The attack was attributed to a ransomware group targeting financial institutions.
7. Between 2023 and 2025, a U.S. financial regulatory agency experienced a prolonged cybersecurity incident involving a compromised internal administrative email account. Unauthorized actors accessed approximately 150,000 emails, with evidence suggesting the intrusion went undetected for over a year. The exposed communications contained highly sensitive supervisory information.
8. In 2025, a cyberattack targeting a third-party technology provider in the mortgage services ecosystem resulted in the potential exposure of sensitive customer information. Compromised data included Social Security numbers and detailed financial records across multiple large institutions. The incident highlighted significant supply chain risks and prompted a federal law enforcement investigation.



READY TO GET STARTED?

Visit **blackbox.com** today.

Black Box® is a trusted IT solutions provider delivering cutting-edge technology products and world-class consulting services to businesses across the globe in every industry. The breadth of our global reach and depth of our expertise accelerate customer success by bringing people, ideas, and technology together to solve real-world business problems.