KATALYST

DIGITAL OPERATIONS PARTNER

CREDIT UNION EDITION

2026 Katalyst Cybersecurity Executive Report

Securing Your Digital Backbone

How Credit Unions Are Reducing Risk, Simplifying Vendor Sprawl, and Operating with Greater Resilience in 2026

Credit unions operate at the intersection of member trust and regulatory accountability. The NCUA has made clear that cybersecurity is an examination priority — and member-owned institutions face the same threat landscape as large banks with a fraction of resources and budget. The credit unions pulling ahead treat their Digital Backbone as a strategic asset, not an operational overhead.

This report is your benchmark. Your baseline. Your starting point.

$6M+
avg breach cost

168 days
avg time to detect

94%
ransomware exfiltrates data

73%
of credit unions cite cybersecurity as a top concern

EXECUTIVE LETTER

A Message From Our CEO

Something has shifted in the conversations I have with credit union leaders. They are no longer asking whether cybersecurity matters to member trust. They are asking why it feels so hard to get under control, and what it will take to get ahead of it.

- **Member trust is now a security outcome**
- **Boards and supervisory committees are asking different questions**
- **NCUA examination scrutiny is accelerating**
- **Growth and core modernization are colliding**
- **Vendor and CUSO sprawl is compounding exposure**
- **Internal bandwidth has reached its limit**

The credit unions that solve this in 2026 carry a durable advantage forward. They protect member trust, walk into NCUA exams with documented evidence, and keep digital services running. The ones that don't keep paying in breach costs, exam findings, staff burnout, and the member confidence they cannot easily rebuild.

Luke Johnson
CEO, Katalyst
Digital Operations Partner

The conversation in every credit union boardroom has changed. Technology risk is no longer a footnote in the annual report. It is a standing agenda item in supervisory committee and board meetings across institutions of every size, because when systems go down, member trust is what is on the line.

> *"The Digital Backbone must be intentional. It cannot be inherited, assembled by accident, or managed by whoever has time."*

What does that mean in practice? It means the infrastructure your institution depends on, the network, the core and digital banking platforms, the cloud environment, and the Microsoft 365 platform your staff work in every day, needs to be owned, operated, and improved with the same discipline you apply to protecting members' money.

Security is a discipline, not a purchase.

The credit unions pulling ahead are not those with the most tools. They have the clearest accountability and the most consistent execution.

Compliance is a floor, not a ceiling.

NCUA examiners, insurers, and members are raising expectations faster than most institutions are raising their posture. Exam readiness is the baseline, not the goal.

The co-managed model is how this gets solved.

Credit unions cannot hire their way to security maturity. Embedded partnership with shared accountability is the answer.

Six Forces Reshaping Technology Leadership

Credit unions are balancing growing cybersecurity threats, evolving member expectations, regulatory scrutiny, and operational efficiency, all while protecting trust. These are six forces reshaping technology leadership in 2026.

01

Security Leadership Has Changed

Cybersecurity is now a board-level responsibility. Technology leaders are expected to demonstrate operational resilience, manage enterprise risk, and communicate cybersecurity as a business priority, not simply an IT function.

02

Third-Party Risk Expectations Are Increasing

Examiners, business partners, and technology vendors increasingly expect documented security controls, vendor oversight, and demonstrable risk management. Managing third-party relationships has become a critical component of operational resilience.

03

Vendor Ecosystems Are Becoming More Complex

Core platforms, digital banking, payment systems, fintech partnerships, and cloud services continue to expand the technology ecosystem. Every new integration introduces operational dependencies, security considerations, and vendor risk.

04

Technology Priorities Continue to Expand

Technology teams are balancing cybersecurity, member experience, AI adoption, infrastructure modernization, and regulatory expectations, all while maintaining day-to-day operations. Strategic priorities increasingly compete for the same resources.

05

Member Trust Has Become a Competitive Advantage

Members expect secure digital banking experiences, uninterrupted access, and responsible stewardship of their personal information. Cybersecurity is no longer just a technical investment. It directly influences member confidence and institutional reputation.

06

Digital Transformation Is Expanding Risk

Digital banking, cloud adoption, fintech partnerships, hybrid work, and evolving member expectations continue to expand the attack surface. Growth initiatives require security to be integrated from the beginning, not added later.

EXECUTIVE LETTER

A Different Conversation Is Happening in Credit Union Boardrooms

- Member data protection
- NCUA examination readiness
- Vendor/CUSO risk exposure
- Digital service continuity
- Reputational and fiduciary risk

In 2026, cybersecurity is no longer an IT conversation at credit unions. It is a supervisory committee and board-level accountability — one where NCUA examiners expect documented evidence, not good intentions.

57% of financial institutions say cybersecurity staffing shortages increase risk

80% of organizations experienced identity-related security incidents in the last year

68% of CISOs now report directly to executive leadership or the board

The credit unions that move from reactive compliance to intentional digital backbone management are gaining something more valuable than exam readiness:

Confidence.

1 in 4
credit unions report material third-party or CUSO risk exposure

2.8B
lost globally to business email compromise and wire fraud

93%
of financial institutions say cyber risk is now a board-level issue

48%
of financial institutions cite vendor risk management as a top security concern

Risk Is Rising. Internal Capacity Is Not.

#3
most targeted industry globally

168 days
avg breach detection time

50%+
of Credit Unions fail to test backups regularly

40+
vendor integrations typical in credit unions

1:50–100
IT staff-to-employee ratio

The issue is not lack of tools. It is lack of operational alignment.

Credit unions are #3 most targeted globally

Member financial data, ACH access, and core banking credentials make credit unions high-value targets. Threat actors do not distinguish by charter type.

NCUA now requires documented security controls

Examination findings cite insufficient MFA, untested backups, and undocumented incident response as top deficiencies. The bar keeps rising.

168 days to detect, 51 more to contain

By the time the breach is confirmed, months of damage are done. Member data has been exfiltrated, credentials sold, and lateral movement completed.

Vendor ecosystems routinely exceed 40+ providers

Core, digital banking, card processing, lending, compliance — each is a potential entry point. Most credit unions have no single view of that exposure.

1 in 4 report material third-party cyber exposure

CUSO relationships, core processors, and fintech integrations create third-party risk that NCUA examiners now actively scrutinize.

Core modernization introduces new integration risks

Each migration or fintech integration creates a new attack surface if it isn't managed with operational discipline throughout the transition.

Identity Is the New Perimeter

Identity

60%+ of breaches involve compromised credentials

Inconsistent MFA enforcement across privileged accounts remains common across credit unions of all asset sizes. Identity maturity now directly correlates with NCUA examination outcomes and cyber insurance eligibility.

Access rights reviews, conditional access policies, and privileged account governance are no longer optional — they are documented examination expectations.

Credit unions that have operationalized identity controls are passing exams cleaner, qualifying for better insurance terms, and responding to incidents faster.

Email

75% of attacks originate through email

AI-driven phishing has dramatically increased impersonation sophistication — particularly targeting CEO, CFO, and lending officer communications at credit unions.

Wire transfer fraud and ACH manipulation via business email compromise continue to increase. Email security without continuous tuning leaves significant gaps that examiners now test for.

Member-facing email channels add additional exposure. Impersonation of credit union staff to reach members is an escalating threat vector that requires both technical and awareness controls.

73%
of financial institutions fail to test backups regularly

MFA
now an NCUA exam expectation

83%
of phishing emails now incorporate AI-generated content

2.8B
lost to BEC scams in 2025

Recovery Is a Strategic Function

Nearly half of credit unions reviewed had not conducted documented restore testing within the past 12 months.

94%

of ransomware incidents include data exfiltration

Credit unions without immutable backups are more likely to pay ransom.

When a ransomware event hits and backups are unavailable or untested, the calculus shifts fast. Immutable, tested, segmented backups remove that leverage entirely — and satisfy examiner expectations.

Backups alone are not protection. Tested, segmented, immutable backups are protection.

The backup job completing successfully is not the same as the backup restoring successfully. Quarterly restore tests — documented and reviewed by management — are the NCUA-expected standard.

50%

of organizations fail to test backups annually

RTO and RPO must be documented, tested, and achievable.

Aspirational recovery numbers on a policy document are not the same as validated recovery capability. If your RTO and RPO haven't been tested in the past 12 months, you don't know if they're real.

Complexity Increases Cost. Katalyst Reduces It.

> *"I've been impressed with the partnership Katalyst has provided since day one. When our network outage hit, their team jumped in with experience and keen troubleshooting skills."*
>
> — SVP of IT Operations, $2B+ Mid-Atlantic Credit Union

1

No Unified Visibility

3–5 overlapping security vendors. Separate dashboards for firewall, endpoint, email, and core. No single view of what you have.

When something goes wrong, you learn about it from the vendor notification — not your own monitoring. That is the accountability gap.

How Katalyst Helps:

Centralized visibility and operational ownership create a single view across security, infrastructure, identity, and core systems. Teams stop managing disconnected alerts and start operating from a unified environment.

2

Examination Fatigue

No centralized reporting cadence. Controls exist on paper but haven't been validated. Examiners receive inconsistent answers.

NCUA examinations become projects you execute before the exam rather than a posture you demonstrate continuously.

How Katalyst Helps:

Continuous validation, reporting, and operational governance reduce last-minute audit preparation and create more consistent examiner outcomes year-round.

3

Operational Drift

Without ownership, environments degrade quietly. What was configured correctly gets changed. No one notices until something breaks.

The most dangerous gaps aren't the ones you know about. They're the controls that worked last year and stopped working when nobody was watching.

How Katalyst Helps:

Defined ownership and continuous oversight prevent environments from slowly degrading over time. Configuration, policy, and security standards stay aligned as systems evolve.

3–5
overlapping security tools common

40+
vendor integrations typical in credit unions

0
single owners of the full environment

AI Is Not a Future Problem. It Is a Present Multiplier.

AI-Generated Phishing

AI-generated phishing campaigns are becoming more convincing, personalized, and difficult to detect across credit union operations.

Attackers use AI to mimic executives, employees, trusted vendors, and member communications. Technical controls remain essential, but ongoing security awareness training is becoming equally important.

Deepfake Impersonation

AI-generated voice and video are making executive impersonation and payment fraud easier than ever.

Fraudsters are using increasingly realistic voice and video impersonation to manipulate payment approvals, account changes, and employee actions. Verification procedures and identity controls are becoming critical safeguards.

AI-Powered Vulnerability Discovery

AI is dramatically reducing the time between finding vulnerabilities and exploiting them.

New AI-powered vulnerability discovery tools can identify weaknesses and generate exploit paths in hours instead of weeks. Organizations relying on periodic scans or inconsistent remediation are increasingly at risk of falling behind.

AI isn't just creating new threats. It's dramatically accelerating how quickly attackers can exploit existing ones.

Recent demonstrations from AI-powered vulnerability discovery platforms such as Mythos show that vulnerability discovery and exploit development can now happen in hours instead of weeks. Credit unions need an ongoing vulnerability management program to continuously identify, prioritize, and remediate risk before attackers can take advantage.

The Risk to Credit Unions Is Immediate

AI is increasing the speed, scale, and sophistication of attacks targeting credit unions. Institutions are seeing more AI-generated phishing, executive impersonation, credential theft, synthetic identity fraud, and AI-powered vulnerability discovery. At the same time, employees are increasingly using public AI tools without understanding the security implications, creating new avenues for sensitive data exposure. Credit unions that combine security awareness training, secure access controls, behavioral monitoring, centralized visibility, and a mature vulnerability management program are significantly better positioned to reduce risk before attacks affect members or disrupt operations.

Security Awareness Training

Build a security-aware culture through ongoing phishing simulations, end-user education, and reporting workflows that help employees recognize evolving AI-powered social engineering attacks.

Secure Access (SASE)

Protect sensitive member information by applying consistent access policies, web filtering, and data controls across users, devices, and cloud applications. This also helps reduce risk from Shadow AI and unintended data exposure.

Managed Security Services

Behavioral monitoring, anomaly detection, and centralized visibility across identity, email, endpoints, and infrastructure enable faster detection and response before threats impact members or operations.

Vulnerability Management

Continuously identify, prioritize, and remediate vulnerabilities across your environment to reduce the growing window of exposure created by AI-powered discovery tools.

The Accountability Gap Is Not Tool Access. It Is Operational Discipline.

High Performers

- **MFA enforced across 95%+ of privileged accounts**
  Not just enabled — enforced, monitored, and reviewed against the full privileged account list every quarter.
- **Documented quarterly backup testing**
  Restore tests are scheduled, executed, and results reviewed by management — not filed and forgotten.
- **24/7 monitoring coverage**
  Active detection, triage, and response capability with defined escalation paths and SLAs.
- **Formalized vendor/CUSO risk review cadence**
  Third-party and CUSO exposure assessed on a schedule, not reactively after an exam finding surfaces.
- **Board-level security reporting**
  The supervisory committee and board receive metrics reflecting actual posture — not just tools purchased.

Lower Performers

- **Rely on ad-hoc monitoring**
  Alerts exist, but no one is consistently accountable for acting on them. Threats persist unnoticed.
- **Test backups irregularly or not at all**
  The backup job ran. Whether it actually restores within the required window is an open question.
- **Maintain overlapping vendor tools**
  Multiple products, none fully owned. Coverage gaps hide in the overlap that nobody reconciles.
- **Address vulnerabilities reactively**
  Patches applied after incidents rather than against a defined SLA tied to severity levels.
- **No structured reporting to supervisory committee**
  Leadership is accountable for risks they can't see. Incidents become the first time the board hears about a gap.

Moving from Examination Readiness to Operational Confidence

FROM

Tool Accumulation

Security, infrastructure, and operational tools are added over time without centralized oversight, creating overlapping functionality, alert fatigue, and growing operational complexity.

TO

Operational Discipline

The goal is not more tools. It is fewer, better-managed tools with clear ownership, tested controls, and measurable outcomes.

FROM

Vendor Sprawl

Multiple vendors managing different parts of the environment create fragmented visibility, inconsistent accountability, and slower response when issues arise.

TO

Strategic Consolidation

CUSO and vendor risk is now an exam priority. Consolidation improves visibility, reduces cost, and creates clear accountability.

FROM

Reactive Fixes

Technology and security gaps are often addressed only after audits, outages, or incidents occur, forcing teams into short-term remediation instead of long-term improvement.

TO

Structured Roadmaps

Responding to exam findings is necessary. Preventing them with a documented, prioritized roadmap is the difference maker.

FROM

IT Isolation

Technology risk is treated as an IT issue instead of an operational and institutional priority, limiting alignment across leadership, compliance, and business strategy.

TO

Board & Committee Alignment

Technology risk is institutional risk. The supervisory committee and board need to own it, not just receive reports about it.

Confidence is built through structure, not urgency.

Resilience Is Built Intentionally

High-performing credit unions treat their technology environment as a unified digital backbone — not a collection of disconnected tools. A resilient backbone is designed with intent, operated with discipline, and improved continuously.

01 CONNECT

Hybrid infrastructure, cloud platforms, and network connectivity managed as one cohesive environment. From on premises infrastructure and Azure to SD WAN, branch offices, and remote access, Katalyst standardizes, monitors, and optimizes how everything connects. Katalyst is accountable for keeping the digital backbone connected, stable, and operational end to end.

- SD-WAN & Networking
- Cloud Connectivity
- Branch & Remote Access
- Managed Infrastructure

02 PROTECT

Security is not a standalone product. It is an operational discipline. Katalyst aligns identity controls, endpoint protection, email security, compliance requirements, monitoring, and incident response into one managed security posture. Katalyst is accountable for continuously reducing risk, validating controls, and strengthening resilience across the environment.

- Identity & MFA
- EDR & Endpoint
- Email Security
- MDR
- Cybersecurity
- Compliance
- MSSP
- SIEM

03 OPERATE

24/7/365 operational management backed by strategic guidance and measurable accountability. Katalyst provides continuous monitoring, help desk support, Microsoft 365 management, backup validation, security oversight, and operational reviews focused on ongoing improvement. Katalyst is accountable for helping organizations operate more efficiently, recover faster, and continuously strengthen their digital backbone over time.

- Help Desk
- Backup & DR
- Microsoft 365
- Advisory & QBRs
- vCIO
- Managed Security
- Managed Infrastructure

The backbone is not about adding tools. It is about operating them intentionally.

A Practical Roadmap for 2026

1 Immediate
0–90 Days

- **Review Identity and Access Management (IAM)**

  Review how identities are managed across employees, administrators, third-party vendors, and remote access. Verify MFA is consistently enforced, validate privileged access, and identify inactive or unnecessary accounts that increase risk and examination findings.

- **Conduct CUSO and vendor exposure review**

  Map your top 10–15 vendors and CUSOs by data access level. Assess what security controls you have visibility into and which relationships lack a formal review process.

- **Validate backup testing documentation**

  Pull the last restore test record. Confirm it covers core systems. If you can't find it or it's more than 90 days old, that is the first thing to fix before your next NCUA exam.

2 Mid-Term
3–6 Months

- **Implement a Vulnerability Management Program**

  Establish a consistent process to identify, prioritize, and remediate vulnerabilities across your environment. Continuous vulnerability management improves operational resilience and helps demonstrate a mature cybersecurity program during examinations.

- **Standardize reporting cadence**

  Establish a monthly security metrics report for management and a quarterly posture brief for the supervisory committee. Both should show movement, not just status.

- **Align IT roadmap with NCUA guidance categories**

  Map your planned work against NCUA cybersecurity guidance. Every initiative should have an owner, a timeline, and a link to a known risk or examination expectation.

3 Long-Term
6–12 Months

- **Establish digital backbone governance model**

  Define clear ownership for Connect, Protect, and Operate domains. Establish accountability, performance metrics, and regular governance reviews that help leadership measure progress and address risk over time.

- **Embed structured resilience testing**

  Schedule tabletop exercises, backup restore tests, and IR simulations on the annual calendar. Make them mandatory, documented, and reviewed by the supervisory committee.

- **Continuously Align Board Reporting with Operational Metrics**

  Supervisory committee reporting should demonstrate measurable improvements in cybersecurity posture, operational resilience, and risk reduction. Regular reporting should help leadership make informed decisions, not simply satisfy examination requirements.

Ready to strengthen your digital backbone? Schedule a conversation with Katalyst.

KATALYST

DIGITAL OPERATIONS PARTNER

Your Digital Backbone. Owned. Operated. Continuously Improved.

katalystng.com
704-790-4440
Charlotte, NC | Spartanburg, SC

Assess.
Benchmark your environment across Connect, Protect, and Operate.

Transform.
Build and execute a practical, prioritized roadmap.

Manage.
Ongoing ownership, visibility, and continuous improvement, 24/7/365.

> *"The Katalyst team found creative ways to consolidate multiple services into one package offering, reducing our expenses by 36%."*
>
> **Chris Libby · Director of IT, Spero Financial**

> *"Our clients trust us as advisors, and having a partner we trust to support infrastructure, security, and IT operations is a huge win for credit unions."*
>
> **Damon Sipe · CTO, Engage FI**

> *"From start to finish, Katalyst goes the extra mile to make sure you are taken care of."*
>
> **Jimmy Dickson · VP of Information Security, All South Federal Credit Union**

SOURCES & REFERENCES

1. IBM Cost of a Data Breach Report – Financial Services Sector
2. Industry Email Threat Reports 2025–2026
3. Ransomware & Data Exfiltration Research 2025
4. NCUA Cybersecurity Guidance & Supervisory Priorities 2025–2026
5. Third-Party / CUSO Risk Exposure Studies 2025
6. Cyber Insurance Underwriting Requirement Reports
7. Ransomware Recovery & Backup Studies
8. AI Phishing & Impersonation Threat Analysis
9. IBM Cost of a Data Breach – Mean Time to Identify & Contain, 2024

This report is produced by Katalyst for informational purposes. Statistics sourced from publicly available industry research. Verify against primary sources before formal reporting.

Digital Backbone Assessment

Benchmark your full environment across Connect, Protect, and Operate.

30-Day Satisfaction Guarantee

If we're not delivering, we make it right or we refund you.

Start the Conversation

katalystng.com · 704-790-4440
Charlotte, NC | Spartanburg, SC