KATALYST

DIGITAL OPERATIONS PARTNER

SLED EDITION

2026 Katalyst Cybersecurity Executive Report

Securing Your Digital Backbone

How State, Local, and Education Organizations Are Protecting Public Services and Strengthening Their Digital Backbone in 2026

SLED organizations operate the services that communities depend on: including but not limited to, emergency response, payroll, public records, school infrastructure, utility systems, and citizen portals. When technology fails, citizens feel it. In 2026, public-sector entities remain among the most targeted by ransomware actors. The organizations building resilient digital backbones are reducing disruption risk while maintaining the transparency and accountability their communities depend on.

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

Top 5
most ransomware-targeted sector

168 Days
days on average to detect a breach

94%
of ransomware exfiltrates data

CJIS
CJIS / FERPA compliance focus 2026

EXECUTIVE LETTER

A Message From Our CEO

Something has shifted in the conversations I have with public-sector leaders. They are no longer asking whether cybersecurity matters to the communities they serve. They are asking why it feels so hard to get under control, and what it will take to get ahead of it.

- **Downtime now disrupts public services, not just IT**
- **Elected leaders and boards are asking different questions**
- **CJIS, FERPA, and grant mandates are accelerating**
- **Aging systems and modernization are colliding**
- **Vendor and inter-agency sprawl is compounding exposure**
- **Budgets and staffing have reached their limit**

The agencies and districts that solve this in 2026 carry a durable advantage forward. They protect public services, meet grant and compliance requirements with documented evidence, and keep critical systems running. The ones that don't keep paying in downtime, lost grant funding, staff burnout, and the public trust they cannot easily rebuild.

Luke Johnson
CEO, Katalyst
Digital Operations Partner

The conversation in every council chamber and board room has changed. Technology risk is no longer a footnote in the annual report. It is a standing agenda item in leadership and oversight meetings across organizations of every size, because when systems go down, the community is what feels it.

> *"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 organization depends on, the network, the systems behind emergency response, payroll, and public records, 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 the public expects of every service you deliver.

Security is a discipline, not a purchase.

The agencies pulling ahead are not those with the most tools. They have the clearest accountability and the most consistent execution across every department.

Compliance is a floor, not a ceiling.

CJIS, FERPA, grant funders, and the communities you serve are raising expectations faster than most organizations are raising their posture. Compliance is the baseline, not the goal.

The co-managed model is how this gets solved.

Public-sector organizations cannot hire their way to security maturity, especially under budget pressure. Embedded partnership with shared accountability is the answer.

THE EXECUTIVE SHIFT IN 2026

Six Forces Reshaping Technology Leadership

State and local governments and educational institutions are balancing growing cybersecurity threats, aging infrastructure, public service demands, and increasing digital expectations. These are six forces reshaping technology leadership in 2026.

01

Security Leadership Has Changed

Cybersecurity has become an executive responsibility. Technology leaders are expected to protect critical services, manage organizational risk, and strengthen operational resilience, not simply support IT operations.

02

Third-Party Risk Is Expanding

Government agencies and educational institutions rely on software vendors, cloud providers, managed service partners, and technology contractors to deliver essential services. Managing third-party risk has become critical to protecting operations and public trust.

03

Connected Public Services Are Expanding Risk

Cloud platforms, public-facing applications, remote access, connected facilities, and critical infrastructure continue to expand the technology ecosystem. Every new connection introduces additional cybersecurity and operational risk.

04

Technology Priorities Continue to Expand

Technology teams are balancing cybersecurity, modernization initiatives, AI adoption, infrastructure improvements, and daily operational support while maintaining essential public services. Strategic priorities increasingly compete for the same resources.

05

Operational Resilience Supports Public Trust

Service disruptions, ransomware, and technology outages directly affect citizens, students, employees, and community services. Operational resilience has become essential to maintaining public trust.

06

Digital Government Is Expanding the Attack Surface

Cloud adoption, hybrid work, connected facilities, AI-enabled services, and expanding digital citizen services continue to increase the attack surface. Security should be integrated into modernization efforts from the beginning.

EXECUTIVE LETTER

Public Trust Depends on Digital Stability in SLED Organizations

- Emergency response continuity
- Public records protection
- CJIS, FERPA & state mandate compliance
- Grant-funded security requirements
- Vendor & third-party risk exposure

In 2026, cybersecurity is not an optional budget line for SLED organizations. It is the foundation of public trust. When systems go down, communities lose access to emergency services, payroll fails, records become inaccessible, and schools cannot teach.

52% of public sector organizations cite staffing shortages as a top cyber challenge

74% of agencies operate legacy or unsupported systems

21 days average public sector downtime

The agencies that move from reactive incident response to intentional digital backbone management are gaining something their communities depend on:

Confidence.

43%
cite budget constraints as a top cyber barrier

67%
of agencies lack 24/7 security monitoring

1 in 3
public sector organizations hit by ransomware annually

40+
systems & vendors managed across departments

Expanded Risk. Limited Resources.

Top 5
most targeted sectors for ransomware

75%
of public entities experienced cyber incidents in the past year

45%
of agencies lack dedicated cybersecurity staff

74%
of agencies operate legacy or unsupported systems

$1.2M
avg recovery cost for municipal ransomware incidents

Security modernization is necessary. But it must align with funding realities and operational constraints.

Aging infrastructure + growing threat sophistication

Many SLED environments run legacy systems that were never designed with modern threat vectors in mind. Attackers know this, and they target it specifically.

CJIS, FERPA, and state mandates require documented compliance

Criminal justice data, student records, and financial systems each carry specific regulatory obligations. Non-compliance exposes both the agency and the individuals whose data was entrusted to it.

Decentralized departments create fragmented security posture

Sometimes when departments manage their own IT, there is no unified view of exposure. Configuration drift, inconsistent controls, and competing vendors make monitoring nearly impossible.

Ransomware has already hit police departments, school districts, and county offices

These are not theoretical risks. Public-sector ransomware incidents have disrupted 911 systems, cancelled school days, and suspended payroll processing for weeks at a time.

Grant funding increasingly tied to demonstrable security controls

FEMA, COPS, E-Rate, and state cybersecurity grants now require documented evidence of security posture. Organizations without it are leaving money on the table.

Third-party and vendor exposure is increasing

Public-sector environments rely on managed service vendors, software providers, cloud platforms, and regional IT cooperatives. A breach in any of those creates cascading impact across agencies.

WHERE RISK IS ACTUALLY EMERGING

Identity Is the New Perimeter

Identity

60%+ of breaches involve compromised credentials

Administrative staff, finance departments, and leadership are frequent phishing targets in SLED environments. Without strong identity governance, a single compromised credential can provide system-wide access across departments, including criminal justice systems, payroll, and student records. MFA enforcement is now an explicit expectation in CJIS policy and emerging state cybersecurity standards. Organizations that haven't operationalized identity controls are failing audits and losing grant eligibility. Access rights reviews, conditional access policies, and privilege management are no longer optional. They are the baseline that regulators, grant administrators, and insurers expect to see documented.

Email

75% of attacks originate through email

Phishing continues to be the primary entry point for public-sector breaches. Finance departments are targeted for fraudulent wire transfers. School administrators are impersonated to reach students and parents. Elected officials are targeted for credential theft. AI-driven phishing has dramatically increased sophistication. Messages now reference real colleagues, upcoming board meetings, and grant applications, making them nearly indistinguishable from legitimate email. Email security without continuous tuning leaves significant gaps. A configuration set in 2023 does not reflect the threat landscape of 2026.

48%
of agencies operate legacy or unsupported systems

CJIS
mandates MFA for criminal justice access

74%
of agencies operate legacy systems

E-Rate
grant security requirements continuing to expand

Recovery Is a Strategic Function

72+

Hours

avg municipal system recovery time after ransomware

61%

of public entities lack tested recovery plans

Many SLED organizations reviewed had not conducted documented restore testing within the past 12 months, even those with active backup systems.

In SLED, downtime is not a business metric. It is a public service failure.

When a county system goes offline, payroll stops. When a school district loses access to its systems, learning stops. When an emergency response system fails, public safety is directly at risk. Recovery time is measured in community impact, not SLA credits.

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

The backup job completing successfully is not the same as the backup restoring successfully. Quarterly restore tests that are documented and reviewed by leadership are the standard that grant administrators, auditors, and state regulators now expect to see.

Cross-department recovery coordination is often the missing piece.

SLED environments span multiple departments, locations, and system owners. A backup strategy that covers IT infrastructure but not the systems used by public works, courts, or schools is an incomplete recovery plan regardless of the technology used.

Complexity Increases Cost. Katalyst Reduces It.

> *"I would highly recommend Katalyst Managed Services. It is certainly beneficial to have a qualified vendor monitoring and supporting your environment. It's all about relationship. The Katalyst team listens to what I need and are there to support me. "*
>
> -- Matthew Dull, Director of Information Technology, City of Kings Mountain

1

No Unified Visibility

Department-by-department IT decisions mean multiple firewall vendors, inconsistent endpoint security, and no single view of what is exposed across the organization.

When something goes wrong, leadership learns about it after the fact through a vendor notice, a news report, or a citizen complaint. That is not a security posture. That is absence of one.

Operational Shift:

Centralized visibility across departments, infrastructure, security, and public-facing systems creates a unified operational picture. Agencies move from reactive issue discovery to proactive monitoring and coordinated response.

2

Budget Inefficiency

Fragmented environments duplicate costs. Multiple vendors for the same function, inconsistent licensing, and reactive spending replace the structured investment a unified backbone enables.

SLED organizations often have less budget flexibility than private-sector peers. Fragmentation makes every dollar less effective, while making grant funding harder to justify and document.

Operational Shift:

Strategic consolidation reduces overlapping vendors, inconsistent licensing, and reactive spending. Technology investments become easier to justify, manage, and align to operational priorities and grant requirements.

3

Compliance Complexity

Decentralized IT creates inconsistent compliance posture. CJIS, FERPA, and state mandates apply across all departments, but enforcement gaps in any one of them create agency wide exposure.

Auditors and grant reviewers assess the whole organization. An island of compliance surrounded by unmanaged systems is not passing examination. It is deferring the consequence.

Operational Shift:

Standardized governance, documented controls, and centralized oversight create more consistent compliance across departments. Agencies improve audit readiness while reducing gaps created by decentralized operations.

5–10
departments managing technology independently

40+
systems & vendors common across agencies

0
single owners of agency-wide visibility

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 public-sector organizations.

Attackers use AI to mimic executives, department leaders, procurement teams, trusted vendors, and public-facing 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, vendor requests, 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 delayed 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. Public-sector organizations need an ongoing vulnerability management program to continuously identify, prioritize, and remediate risk before attackers can take advantage.

The Risk to Public-Sector Organizations Is Immediate

AI is increasing the speed, scale, and sophistication of attacks targeting state and local governments and educational institutions. Organizations are seeing more AI-generated phishing, executive impersonation, credential theft, ransomware, 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 citizen data, student information, and organizational data to be exposed.

Public-sector organizations 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 disrupt essential services or erode public trust.

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 attacks targeting public-sector organizations.

Secure Access (SASE)

Protect citizen data, student information, and organizational assets by applying consistent access policies, web filtering, and data controls across users, devices, cloud applications, and remote access. 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 critical infrastructure enable faster detection and response before incidents disrupt essential public services.

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 all departments and remote access**
  Not just enabled on some systems, but enforced consistently across staff, vendors, and all remote connections.
- **Documented quarterly backup and restore testing**
  Restore tests are scheduled, executed, documented, and reviewed by leadership, not filed and forgotten.
- **Centralized 24/7 monitoring coverage**
  Active detection across all departments with defined escalation paths and documented response procedures.
- **Standardized firewall and endpoint platforms**
  Consistent security stack across departments eliminates configuration gaps and simplifies audit preparation.
- **Structured executive and board-level reporting**
  Leadership receives metrics that show actual posture and risk reduction, enabling informed decisions.

Lower Performers

- **Maintain department-specific, inconsistent security stacks**
  Fragmentation hides gaps. What is covered in one department is unprotected in another.
- **Operate reactively by responding to incidents not preventing them**
  Without proactive monitoring, the first sign of a breach is often the impact, not the alert.
- **Lack documented incident response coordination across departments**
  When an incident occurs, no one knows who calls whom, what systems are affected, or what the recovery steps are.
- **Depend on limited internal IT staff without managed support**
  A single IT coordinator handling a multi-department environment is a single point of failure in every direction.
- **No structured reporting to leadership or governing bodies**
  Boards and councils are accountable for decisions they cannot make without visibility. That gap creates liability.

Moving from Vulnerability to Public Resilience

FROM

Dept-by-dept security

Departments and agencies often manage technology independently, creating inconsistent controls, fragmented visibility, and uneven security maturity across the organization.

TO

Unified governance

Security posture should not vary by department. A unified backbone means every agency, office, and school operates under consistent, auditable controls.

FROM

Reactive IT response

IT teams are forced into responding after outages, ransomware events, or user complaints instead of proactively identifying and resolving operational risks before services are disrupted.

TO

Proactive monitoring

SLED organizations cannot afford to learn about incidents after the fact. 24/7 monitoring means threats are identified before they become service disruptions.

FROM

Legacy infrastructure & vendor sprawl

Aging infrastructure, unsupported systems, disconnected platforms, and overlapping vendors create operational complexity and growing security gaps. Inconsistent patching, outdated hardware, and fragmented visibility increase operational risk across the organization.

TO

Strategic modernization

A modernized digital backbone creates standardized infrastructure, consistent patching, supported systems, and centralized visibility across departments and agencies. Reducing technical debt improves resilience, limits vulnerabilities, and closes security gaps before they become operational disruptions.

FROM

Untested backups

Backups may exist, but recovery capability is often assumed rather than validated. Without documented restore testing, agencies cannot confidently measure recovery readiness during a real disruption.

TO

Recovery confidence

A backup that has never been tested is an assumption. Documented quarterly restore testing is the difference between knowing you can recover and hoping you can.

Public trust is built on stability. Stability is built on structure.

Resilience Is Built Intentionally

High-performing SLED organizations treat cybersecurity as infrastructure, not a project. A resilient public-sector digital backbone is designed with intent, operated with discipline, and maintained continuously across departments.

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 MFA enforcement across all departments**

  Audit which systems and users have MFA enforced, not just enabled. Prioritize criminal justice access, finance, and any remote or vendor connections first.

- **Validate backup testing documentation**

  Pull the last restore test record. Confirm it covers all critical systems. If it is more than 90 days old, or you can't find it, that is the first thing to fix.

- **Assess third-party and vendor access**

  Map which vendors have active access to your systems and data. Identify which relationships lack a formal security review or access policy.

2 Mid-Term
3-6 Months

- **Standardize firewall and endpoint platforms across departments**

  Eliminate the patchwork of department-specific tools. Standardization improves monitoring coverage, reduces cost, and strengthens audit documentation.

- **Implement centralized monitoring**

  Establish visibility across all departments from a single platform. Every alert should have an owner, an escalation path, and a documented response.

- **Formalize incident response coordination**

  Document who does what, in what order, when an incident occurs across IT, legal, communications, and department leadership. Practice it before you need it.

3 Long-Term
6-12 Months

- **Establish digital backbone governance model**

  Define clear ownership for Connect, Protect, and Operate across your organization. Document accountability, performance metrics, and the escalation path to leadership.

- **Align cybersecurity roadmap with grant funding opportunities**

  FEMA, COPS, E-Rate, and state cybersecurity grants reward documented posture. Your roadmap should map directly to the evidence these programs require.

- **Introduce structured executive and governing body reporting**

  Leadership cannot govern what they cannot see. Quarterly posture reports that show movement, not just activity, give decision-makers what they need.

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.

> *"They have no problem at all explaining complex IT issues to us. They will sit down and break it down in less-technical language."*
>
> **Allayna Dail · Director of Community Relations, Southport**

> *"I would highly recommend Katalyst Managed Services. It is certainly beneficial to have a qualified vendor monitoring and supporting your environment. It's all about relationship. The Katalyst team listens to what I need and are there to support me. "*
>
> **Matthew Dull · Director of Information Technology, City of Kings Mountain**

SOURCES & REFERENCES

1 Public-Sector Ransomware Research 2025-2026

2 Ransomware & Data Exfiltration Reports 2025

3 Identity Compromise & Phishing Research 2025

4 CJIS Security Policy & Compliance Guidance

5 FERPA Cybersecurity Guidance Updates

6 FEMA / COPS / E-Rate Grant Security Requirements

7 Cyber Insurance Underwriting for Public Sector 2025

8 AI Phishing & Impersonation Threat Analysis

9 IBM Cost of a Data Breach - Government Sector, 2024

Digital Backbone Assessment
Benchmark your full environment across Connect, Protect, and Operate.

Grant Readiness Support
We help document your security posture for FEMA, COPS, E-Rate, and state grants.

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