2026

State of Cyber Security:

Key Insights for Local Governments

Commonwealth Sentinel
Cyber Security

Table of Contents

CONFIDENTIAL

2026 State of Cyber Security:
Key Insights for Local Governments

CONFIDENTIAL

Executive Summary

Local governments enter 2026 facing a threat environment that is faster, more automated, and more disruptive than it was even two years ago. Ransomware remains the most visible risk, but now attacks often involve stealing data and demanding money, even when files aren't locked. Additionally, hackers are working much faster (thanks to the use of AI), often leaving defenders only a few hours or days to detect and react before damage is done.

At the same time, rules and standards for cyber security are getting stricter. The updated NIST Cybersecurity Framework (CSF) now requires leaders to take more responsibility for managing risks and overseeing cyber programs. This is especially important for public-sector organizations, where elected leaders make key decisions about risk and budgets.

CISA is also making it clearer what basic cyber security should look like by updating their performance goals and creating a list of vulnerabilities that should be fixed first. However, many local government don't have enough money or staff to meet these goals, especially in smaller or rural areas.

With recent staffing and budget cuts to CISA and MS-ISAC, and unclear priorities from federal leaders, it seems local governments are going to be left on their own with little or no meaningful support from the state or federal governments.

Key insights for 2026

- Speed matters most. Cyber threats now move quickly, so local governments must spot and stop attacks within hours or days, not weeks.
- Protect logins and accounts. Hackers often break in by stealing passwords or misus-

ing remote access, not just with obvious malware. Keeping accounts safe is crucial.

- Patch the most important vulnerabilities first. Focus on fixing security holes that attackers are actively using. This helps IT teams use their limited time wisely.
- Leadership must get involved. Managing cyber risks is now a core part of running a local government, because these risks can affect public safety, legal matters, and essential services.
- Faster incident reporting is required. Rules are changing so that cyber incidents must be reported more quickly and with more detail. This is becoming standard for critical infrastructure, including local governments.
- Being resilient is better than being perfect. Instead of aiming for flawless security (which is impossible), local governments should focus on detecting and responding to problems fast, limiting damage, backing up data, practicing response plans, and keeping key services running.

This white paper gives local governments a simple, step-by-step plan for 2026 that can work even with limited staff and funding. It includes a clear way to manage cyber security, a list of the most important protections based on the latest CISA and NIST guidelines, and easy-to-follow instructions focused on results and processes that can be used again and again.

Sheri

Sheri Donahue
Cyber Security Evangelist
Co-Founder/CEO
Commonwealth Sentinel
Email: Sheri@CommonwealthSentinel.com
Phone: (502)234-5554
Cell: 502-649-3102

CONFIDENTIAL

The 2026 Threat Landscape for Local Government

http://very.very.legit
X
Check payment
Enter decrypt code
dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur.
Excepteur sint occaecat cupidatat non proident, sunt in culpa qui officia deserunt
mollit anim id est laborum.

ENCRYPTION WARNING!

YOU ARE HACKED

ALL YOUR FILES ARE ENCRYPTED

Your computer is **LOCKED**
and all files will be deleted in 48 hours.
Send $500 worth of bitcoin to specified address.
Authorities will not help you. You will lose your files if you contact them.

SYSTEM ENCRYPTED

1.1 Ransomware and extortion remain the top threats

Ransomware continues to dominate local government headlines because it directly interrupts services: public safety dispatch, court operations, payroll, permitting, utility billing, and public records. The public sector remains a consistent target. Verizon's 2025 public sector analysis notes the presence of ransomware in a significant share of breaches and highlights that local governments account for a substantial share of ransomware victims in the U.S. public sector.

Two key factors for 2026:

- Cyberattacks happen faster than ever. Hackers can move from their first break-in to causing serious problems (like launching ransomware) very quickly, sometimes in less than a week. In recent investigations, most ransomware attacks happened within just a few days of the initial breach.
- Ransom attacks are about more than just locking files. Many criminal groups now focus on stealing sensitive data and threatening to make it public or shame their victims, even if they don't completely encrypt files. This puts pressure on organizations because even reliable backups won't stop the damage from stolen information or public exposure.

1.2 The initial access economy is thriving

The way cyber attackers break into municipal computer networks isn't like what you see in movies. Instead, they use predictable and profitable methods:

- Stolen or misused login information: Attackers get in by tricking people (phishing), reusing passwords, stealing login details, wearing down multi-factor authentication (MFA), or taking advantage of weak remote access.
- Unpatched security holes: Hackers exploit known weaknesses in devices that connect to the internet, VPNs, gateways, or outdated software that hasn't been updated.
- Third-party access: Criminals might get in through outside companies like managed service providers (MSPs), vendors, and those who share services with the municipality.

Top 5 Threats to the Public Sector

- State-sponsored attacks
- Ransomware
- Phishing attacks
- Improper usage
- Internal attacks

Source: The Institute for Defense & Business

- Email scams and business tricks: Attackers use fake emails to fool staff into rerouting payments, diverting payroll, or processing fraudulent invoices (also known as Business Email Compromise (BEC)).

For people defending these networks, the best return on effort is to focus on the basics: securing user identities, quickly fixing (patching) exploited vulnerabilities, segmenting the network to limit damage, protecting backups, and practicing response to incidents.

1.3 AI changes the tempo on both sides

Security experts say that use of AI is helping defenders find and fix problems faster. At the same time, hackers are using AI to trick people and break in more quickly. The practical implication for local governments is not “buy an AI tool.” Instead,focus on these basics:

- Make it easier to spot problems and fix them fast
- Cut down on too many security alerts
- Make sure people review and approve anything risky before it happens

1.4 Known Exploited Vulnerabilities (KEV): The Most Common Way Hackers Get In

The CISA KEV Catalog is explicitly designed as an authoritative list of vulnerabilities being exploited “in the wild,” and CISA recommends every organization should use KEV to decide which issues to fix first. For local governments, KEV should become a standing weekly agenda item for IT/security teams and a monthly reporting line to leadership:

- How many KEVs exist in our computer network?
- How fast are we fixing or patching them?
- Are any of these KEVs on computers that are connected to the internet or critical systems?

CONFIDENTIAL

Cyber Security Leadership in 2026: Making Cyber Leadership a Priority

CONFIDE

2. CSF 2.0 Puts Governance Front and Center

NIST CSF 2.0 introduces "Govern" as a core function alongside Identify, Protect, Detect, Respond, and Recover. This is not just theoretical. It is a direct reflection of what municipal cyber security has become: a balance of risk, services, funding, and accountability.

A local government that treats cyber security as "an IT issue" will continue to face problems that could have been avoided. A local government that treats cyber security as something that affects how services are delivered and how resilient the community is will make smarter choices about:

- How much money to invest
- Upgrading and modernizing technology
- Managing outside vendors
- Making decisions during incidents
- Planning for continuity and recovery

2.2 A Practical Governance Model for Local Governments

A workable governance model for managing cyber security in 2026 has five parts:

1) Executive ownership

- Designate a single accountable executive (CIO/CTO, finance/administration leader, or an appointed security lead) who owns the cyber program outcomes.
- Ensure this person is given the authority to set standards and enforce remediation timelines.

2) Cyber Steering Committee

A monthly committee that includes:

- IT/security leadership
- Finance/purchasing
- Legal/records
- HR/training
- Emergency management/public safety
- Other key department heads (courts, utilities, city/county clerk, etc.)

3) Risk Register and Decision Process

- Maintain a living, prioritized list of cyber risks tied to municipal services (e.g., “911 outage,” “water billing disruption,” “public records leaked”).

- Review top risks quarterly; document acceptance, mitigation, or transfer.

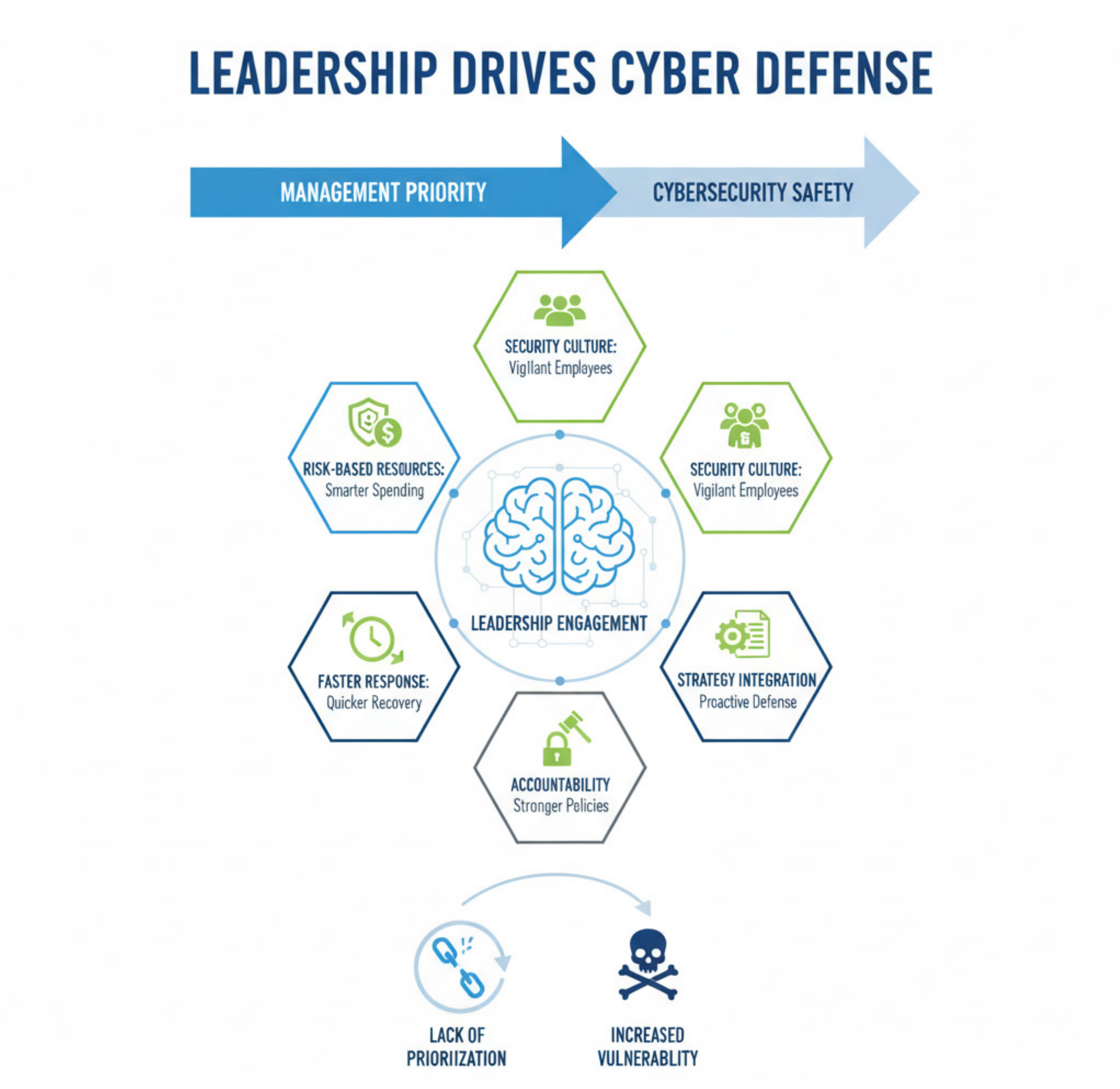
4) Policy Set with Enforcement

Stick to the basics: rules for identity, access, patching, backups, logging, vendor access, and incident response.

5) Leadership Metrics

Leadership does not need every technical detail. They need a dashboard that answers:

- Are we reducing risk over time?
- Are we getting faster at patching?
- Are we more resilient this quarter than last quarter?



Funding and Capability: What Local Governments Can Actually Build

CONFIDE

3. Budget reality: capability gaps persist

MS-ISAC reports show that smaller and rural local governments often don't have enough money or resources to protect themselves from cyber threats. In practice, this means many local governments have:

- Limited staff dedicated to security
- Aging and outdated infrastructure (i.e., computers)
- Inconsistent patching and software updates
- Insufficient logging/monitoring
- Backup and restore processes not tested often enough

This is not the fault of anyone. It is just a reality in local governments and they need to focus on what is most important and build the capabilities piece by piece.

3.2 SLCGP as a strategic lever

The future of the SLCGP is unclear at this time

The State and Local Cybersecurity Grant Program (SLCGP) is one of the most critical funding sources for local governments to scale cyber security improvements. FEMA and CISA created this program to ehelp states and local governments handle and reduce cyber security risks.

In 2026, high-impact grant-aligned investments typically include:

- MFA/identity modernization
- Endpoint hardening and managed detection
- Vulnerability management and patch tooling
- Backup modernization (immutable)
- Incident response planning, tabletop exercises, and training
- Network segmentation and privileged access management
- Logging/SIEM modernization and central monitoring

The strategic mistake is using grant money on "one-off tools" without having enough staff or expertise to use it well.

The 2026 Baseline: Key Cyber Security Controls for Local Governments

CONFIDE

Local governments need a baseline that is specific, measurable, and feasible. CISA's Cybersecurity Performance Goals (CPG) 2.0 are designed as "high-impact" cyber security actions for a foundational level of security and resilience.

Below is a recommended baseline organized into key focus areas. (In Part 2, this is translated into a 12-month implementation roadmap with templates.)

4.1 Identity and access (highest ROI)

Outcomes

- MFA is required and enforced for all remote access and privileged actions.
- Privileged accounts are minimized and closely monitored.
- Vendor (or third-party) access is temporary and tracked.

Minimum actions

- Require and eforce MFA for email, VPN, remote desktop gateways, and admin consoles.
- Disable legacy authentication where possible; reduce password reuse (i.e., require unique passwords).
- Implement role-based access control for critical systems.
- Require separate admin accounts that are not used for daily work.
- Create a vendor access standard: least privilege, expiring access, logging.

4.2 Vulnerability and patch management (Fix critical issues first)

Outcomes

- Critical exploited vulnerabilities are remediated quickly, consistently.
- Internet-exposed systems receive patches faster.
- Leadership can see how quickly vulnerabilities are being fixed.

Minimum actions

- Track exposure to known exploited vulnerabilities and prioritize remediation using CISA KEV guidance.
- Establish patch deadlines:

o KEV/internet-exposed: 7 days or less (based on severity)

o critical internal systems: 14–30 days

o all other systems: 60–90 days (based on risk)

4.3 Backups and recovery (Be ready to bounce back)

Outcomes

- Backups are protected from deletion or encryption by attackers.
- Restore procedures are tested for critical systems.
- Recovery time objectives exist for essential services.

Minimum actions

- Maintain at least one immutable (i.e., cannot be changed) or offline backup copy.
- Use separate credentials for backup credentials and regular admin tasks.
- Test restoring data monthly for some systems, quarterly for critical services.
- Document recovery sequences for core services (email, identity, finance, public safety).

4.4 Logging and detection (Spot problems quickly)

Outcomes

- High-value logs are collected and retained.
- Alerts focus on high-signal events: admin changes, lateral movement indicators, suspicious sign-ins, backup tampering.
- Incident response is consistent and repeatable.

Minimum actions

- Centralize authentication logs (cloud and on-prem identity).
- Log remote access gateways and admin consoles.
- Monitor for abnormal sign-in patterns and privilege escalation.
- Ensure log times are accurate and retention policies are set.

4.5 Email and user risk (Protect against human error)

Outcomes

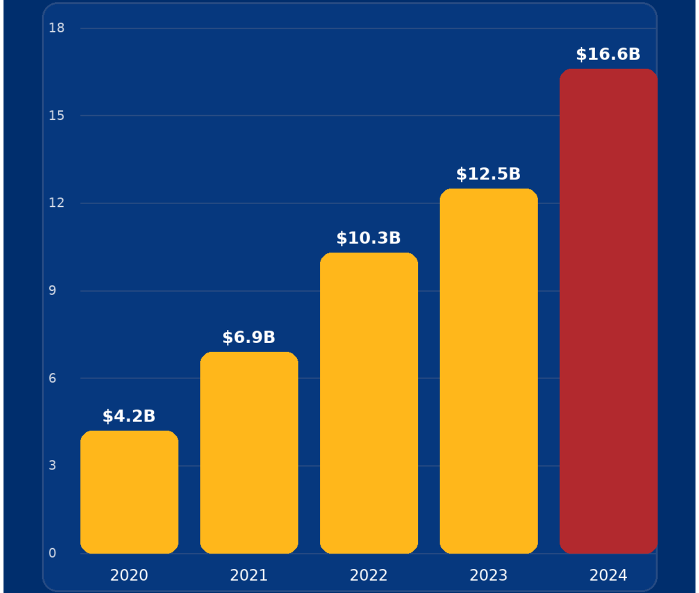
- Phishing success rates decline.
- Staff know how to report suspicious messages and events.
- Business processes reduce fraud likelihood (invoices, ACH changes, payroll).

Minimum actions

- Annual security training; add short, focused training every quarter.
- Set up ways for staff to report phishing and respond quickly.
- Create a “two-channel verification” process for payment changes.
- Align training with observed incidents, not generic content.

CONFIDENTIAL

Reported U.S. Losess to Cyber Crime 2020-2024



Data source: FBI IC3 Annual Reports (2020–2024).

Incident Response in 2026: Building Muscle Memory

CONFIDEN

5.1 Why practiced response is a force multiplier

Since attacker timelines are compressed, being able to respond effectively is less about heroic technical skill and more about:

- Clarity of roles
- Letting the right people act fast to contain the problem
- Clear and reliable communications
- Decision playbooks for worst-case scenarios.

This is especially true in ransomware scenarios, where adversaries may notify victims quickly and force decisions under pressure, mirroring the shorter dwell-time patterns observed in incident data.

5.2 The incident response "minimum viable program"

1) A written incident response plan

- Have a contact list, clearly identify decision authority, describe how to communicate and handle different levels of problems.

2) Pre-negotiated support

- Identify and establish deals with external IR support experts who can help in emergencies (retainer or procurement-ready process).
- Build relationships ahead of time with your cyber insurance providor and legal counsel (if applicable).

3) Tabletop exercises

- Run at least two per year:
  - Ransomware with data theft + service outage
  - Business email compromise + fraudulent payment scenario

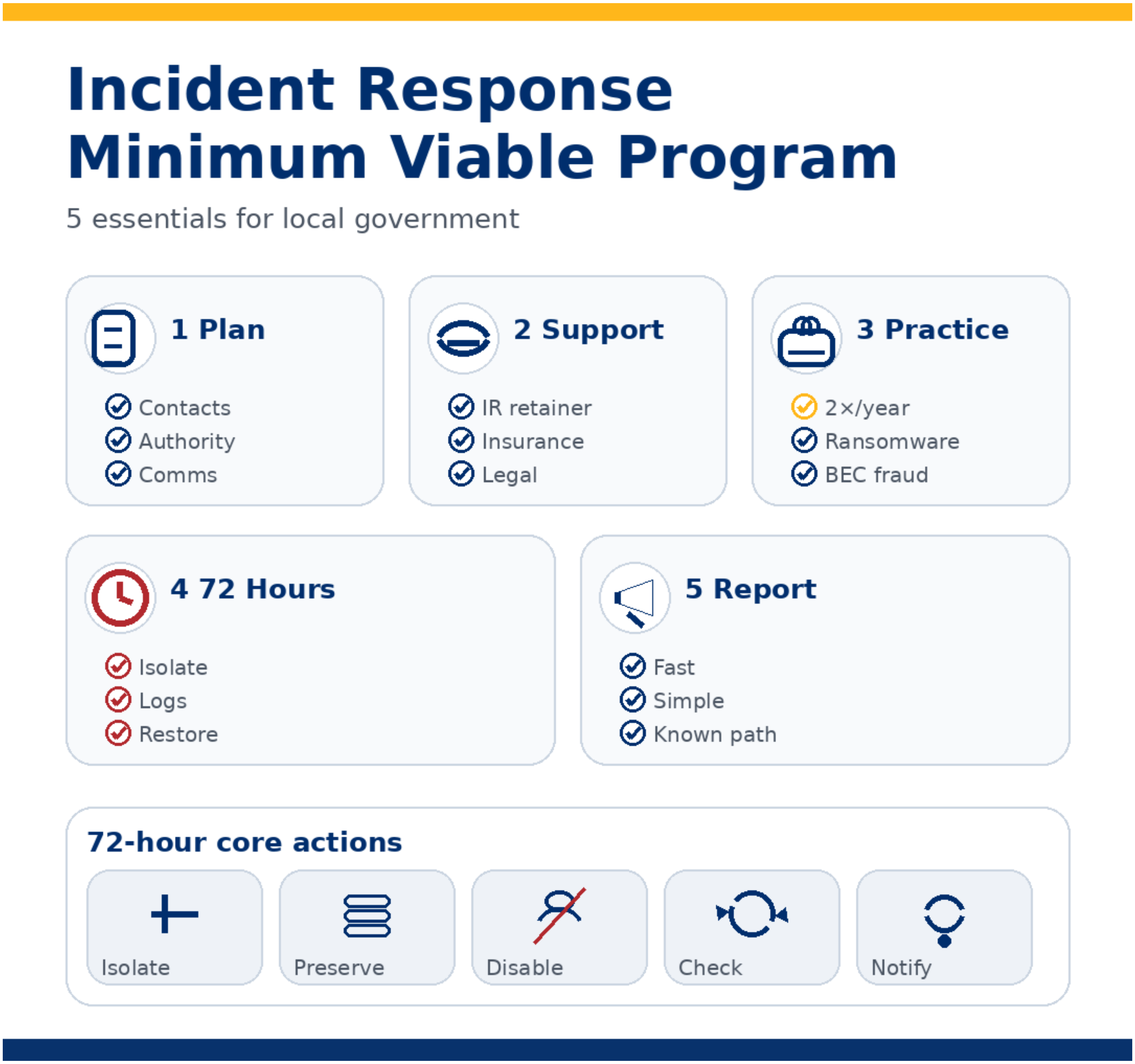
4) A 72-hour operational checklist

- Isolate affected systems
- Preserve evidence/logs
- Disable compromised accounts
- Assess backups and restore viability
- Communicate clearly internally and externally

5) Reporting pathways

- Ensure staff know how to report suspected incidents quickly.

- Align reporting with federal guidance for ransomware reporting (e.g., IC3/FBI reporting encouraged by the FBI and CISA advisories).



Incident Response Minimum Viable Program

5 essentials for local government

1 Plan

- ✓ Contacts
- ✓ Authority
- ✓ Comms

2 Support

- ✓ IR retainer
- ✓ Insurance
- ✓ Legal

3 Practice

- ✓ 2×/year
- ✓ Ransomware
- ✓ BEC fraud

4 72 Hours

- ✓ Isolate
- ✓ Logs
- ✓ Restore

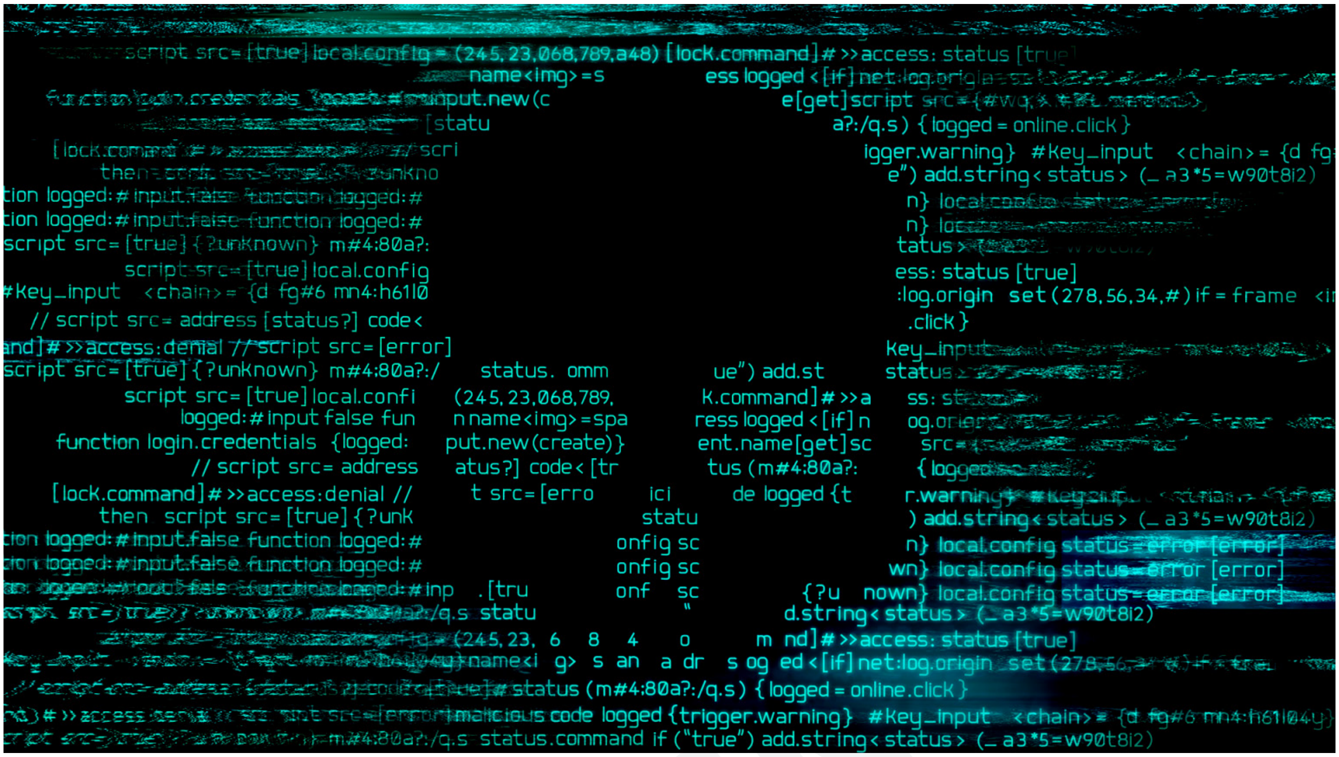
5 Report

- ✓ Fast
- ✓ Simple
- ✓ Known path

72-hour core actions

Isolate | Preserve | Disable | Check | Notify

Incident reporting and compliance: What to Expect in 2026



6.1 CIRCIA: the direction of travel

The rules for reporting cyber security incidents are changing. CISA's Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) program outlines new statutory requirements for organizations to report certain incidents and ransom payments within strict deadlines. Even if a specific local government is not required to follow these rules, they will still feel the effects:

- Vendors and critical infrastructure partners may require faster reporting from you
- State rules may become stricter
- Expectations of timely disclosure and coordination are increasing

Local governments should plan for a future where:

- Reporting deadlines are much shorter
- Documentation standards are higher
- Incident reports must be produced quickly with no ambiguity

6.2 Action for 2026: build a reporting-ready process now

A "reporting-ready" program includes:

- Timestamped incident logs (who did what, when)
- Consistent incident classification system
- Pre-approved external communications templates
- Decision tree for when legal counsel and state/federal partners are engaged

CONFIDEN

A Cyber Security Maturity Model for Local Governments

CONFIDEN

Use this simple maturity ladder to stage improvements without overwhelming the organization:

Level 1: Stabilize

- Use MFA for key systems, regularly update/patch systems, maintain basic backups, provide basic cyber security training, have a basic incident response (IR) plan.

Level 2: Reduce Exposure

- KEV-first patching, remove/secure internet access, privileged access separation from regular users, basic centralized logging, vendor access controls.

Level 3: Improve Detection and Response

- Centralized monitoring, endpoint telemetry, tested backup restoration, IR exercises, refined response playbooks.

Level 4: Build Resilience

Network segmentation, immutable backups, measured recovery times, continuous vulnerability management, and governance dashboards.

CISA’s CPGs, NIST and the CSF 2.0 are good guides for reaching and maintaining these levels in a steady, accountable progression.

Conclusion: What matters most in 2026

For local governments, cyber security in 2026 is about service continuity under adverse pressure. The organizations that perform best are not the ones with the most tools; they are the ones with:

- Strong leadership and decision-making
- KEV-first remediation
- Strong identity management controls
- Protected and tested backups
- Practiced incident response

Commonwealth
Sentinel
Cyber Security

At Commonwealth Sentinel, we stay focused on cyber security so you can focus on other things!

CONFIDENTIAL

Local governments are being targeted by cyber criminals more than ever, and the consequences go far beyond IT: disrupted services, exposed citizens data, and shaken public trust. Commonwealth Sentinel helps you reduce that risk with practical, local-government-focused cyber security that protects the systems your community depends on.

We stay focused on cyber security so you can stay focused on running your offices. From phishing defense and staff training to policy, preparedness, and incident response readiness, we translate complex threats into clear actionable steps that fit real budgets and real staffing.

Commonwealth Sentinel is a partner, not a vendor. We work alongside your leadership and IT team to strengthen day-to-day defenses, improve compliance and resilience, and help ensure that when something happens, you have a plan that keeps services moving and constituents protected.

Are you prepared to take your cyber security to the next level in 2026? We're here to help you make that commitment! When you mention this report you call, we'll offer you a **comprehensive Level 1 Security Scan absolutely FREE!*** Don't miss this opportunity to fortify your defenses. Contact us today!

Sheri

Sheri Donahue
Cyber Security Evangelist
Co-Founder/CEO
Commonwealth Sentinel
Email: Sheri@CommonwealthSentinel.com
Phone: (502)234-5554
Cell: 502-649-3102

* Offer good through April 30, 2026