Building Cyber Resilience Across 26 Local Governments

A white paper based on Hire A Cyber Pro's Kentucky district engagement.

Prepared by: Hire A Cyber Pro LLC

contact@hireacyberpro.com | 865-500-3885 | hireacyberpro.com

October 22, 2025

Executive Summary

Hire A Cyber Pro helped 26 city and county governments in a Kentucky district establish a defensible cybersecurity baseline and prepare for real incidents. Funded by DHS, our team delivered 26 first-time assessments, 25 new incident response plans, and 26 tabletop exercises, giving leaders clarity on risk, readiness, and next steps. We combined NIST 800-30 risk methods, CIS Benchmarks/NIST CSF baselining, the CISA CSET tool, enterprise-grade vulnerability scanning, and external testing to produce actionable roadmaps, POA&Ms, and governance routines. Aggregate risk distribution landed at 22 low-risk, 3 moderate-risk, and 1 high-risk entities, with targeted recommendations for MFA, EDR, patching, email security, logging, MDM, and third-party risk. Outcomes: a consistent starting point across municipalities, better understanding of data at risk, and measurably better incident preparedness.

Context

Industry: Local government (cities/counties).

Regulatory drivers: No prescriptive sector regulation applied; the program's goal was to establish baseline standards aligned to CIS Benchmarks and the NIST Cybersecurity Framework (CSF) so each entity could manage risk coherently and mature over time.

Funding/Alignment: DHS-funded initiative emphasizing community resilience and practical readiness for municipal environments that often rely on small internal teams and/or MSPs.

Top Risks

- Inconsistent Identity & Access Controls — Uneven MFA coverage for email/VPN/admin accounts; privileged account hygiene varied across MSPs and in-house IT.
- Vulnerability & Patch Latency — Legacy systems and deferred reboots left exploitable windows; several entities lacked a formal vulnerability management cadence.
- Limited Telemetry and Response Playbooks — Centralized logging, alerting, and IR runbooks were minimal or ad hoc; many organizations had never run a tabletop exercise before.

Engagement Plan

Phases & Timeline

- Mobilize & Orient (Weeks 1–2): Three virtual group onboarding meetings for all participants; common scope, expectations, data requests, secure evidence exchange.
- Discovery (Weeks 2–8): Leadership interviews; IT/MSP interviews; insurance interviews; OSINT & exposure sweeps (password leaks, dark-web mentions); deploy

sensors for internal vulnerability scanning and asset inventory; external testing of internet-facing services (commercial scanners + manual validation).

- Assessment & Planning (Weeks 6–12): CSET-guided control review; risk analysis (NIST 800-30); POA&M drafting; policy gap mapping to CIS/NIST CSF.
- Exercise & Improve (Weeks 10–20): 26 first-time IR tabletops with custom municipal scenarios; 25 new IR plans completed/approved.
- Governance & Close (Weeks 20–24): Individual read-outs; district-level synthesis; 90-day action plans; cadence for quarterly control checks.

Roles & Governance

- vCISO (Hire A Cyber Pro): Risk method, governance design, policy/plan authorship, executive reporting.
- Security Engineer(s): Scanning, external testing, log/design reviews, technical recommendations.
- Client IT/MSP: Evidence, control configuration, remediation owners.
- Program PMO: Schedule, dependencies, cross-entity issues, metrics roll-up.

What We Did

- Risk Assessment (NIST 800-30): Identify assets/threats/vulnerabilities; estimate likelihood/impact for priority threat events; account for existing mitigations; compute overall risk rating; produce targeted treatments and POA&Ms.
- Control Baseline: CIS Benchmarks + NIST CSF outcomes to harmonize “minimums” across diverse municipalities and MSP arrangements.
- Control Assessment: Structured, evidence-based walkthroughs using the CISA CSET tool to highlight strengths and gaps and to auto-map recommended improvements.
- Technical Testing: External attack surface review (commercial scanners + manual validation); internal vulnerability scanning, asset enumeration, configuration reviews; email/auth hardening where feasible.
- Tabletop Exercises: Customized government-services ransomware scenario (emergency services impact) with injects for communications, decision rights, and recovery operations.

Results

District-Wide Outcomes

- 26 actionable cybersecurity assessments (first-time across municipalities).
- 25 new incident response plans, tailored and approved.
- 26 first-time tabletop exercises completed (executive + technical participants).

Risk Distribution (Baseline)

Risk Level	Entities
Low	22
Moderate	3
High	1

Common Remediation Themes Implemented/Planned

- MFA expansion (email/VPN/admin), EDR deployment, vulnerability/patch cadence, email authentication (SPF/DKIM/DMARC), MDM for mobile endpoints, centralized logging/SIEM with alerting, and third-party/vendor risk practices.

Visuals Produced (per-entity and roll-up)

- Risk heatmap (top 5 risks pre/post).
- POA&M burndown (items closed vs. time).
- Coverage map (MFA/EDR/backup/logging % by entity).

Compliance Outcomes

While not compliance-driven, the program created audit-ready artifacts: IR plans, tabletop evidence, asset/vuln inventories, baseline policies (access control, data protection, incident response), and POA&Ms with owners and due dates. These outcomes align naturally to NIST CSF outcomes and many NIST 800-171 practice areas, accelerating any future state or federal grant reporting and insurer control attestations.

Lessons Learned

- Prepare for Emergency-Services Disruption — Real-world municipal incidents have forced 911/311 dispatch to paper processes; design tabletops that stress public safety continuity and cross-jurisdiction coordination.
- Standardize “Minimums,” Then Iterate — Agreeing district-wide on CIS/NIST CSF baselines and a shared POA&M taxonomy speeds remediation and simplifies MSP coordination.
- Practice Communications as Much as Technology — Tabletops that rehearse decision rights, public messaging, carrier/insurer notifications, and mutual-aid options produce faster, less chaotic responses than purely technical drills.

What's Next

Quarterly Controls & Metrics

- Q1: MFA to 100% of staff/admin paths; privileged access reviews; email authentication enforcement.
- Q2: EDR coverage to 100% of managed endpoints; log centralization with alerting playbooks; backup immutability tests.
- Q3: Patch SLOs by severity (e.g., Critical ≤7 days); configuration hardening to CIS minimums; third-party risk intake.
- Q4: District-wide incident command tabletop (multi-entity), targeted purple-team drills, and annual external testing refresh.

Optimization

- Consolidate overlapping tools; formalize MSP SLAs; expand evidence packs for insurer renewals and future grants.
- Maintain a shared knowledge base (playbooks, runbooks, templates) and a standing PMO for progress tracking.

Training Cadence

- Semiannual executive IR workshops; quarterly technical tabletops; monthly awareness micro-modules.

About Hire A Cyber Pro

Veteran-led cybersecurity firm delivering risk assessments, vCISO services, compliance support (NIST, CMMC, HIPAA), penetration testing, managed vulnerability scanning, SOC-as-a-Service, and more—tailored for municipalities, education, and the public sector. Differentiators: seasoned team, tailored solutions, and continuous support. Contact: contact@hireacyberpro.com • 865-500-3885 • hireacyberpro.com.

References & Notes

- CISA Cybersecurity Evaluation Tool (CSET) — widely used for structured control reviews. https://www.cisa.gov/resources-tools/services/cyber-security-evaluation-tool-cset
- Emergency-services impact examples — recent ransomware incidents have disrupted 911/311 in U.S. cities; use as scenario inspiration for tabletops. https://statescoop.com/columbus-ohio-ransomware-saga-legal-gray-areas-2024/