

From Risk to Readiness: Empowering Kentucky Communities Through Funding and Cyber Confidence

50th Annual Governor's Local Issues Conference

20 August 2026



The better the question. The better the answer. The better the world works.



Shape the future
with confidence

Presenters



Gary Burke
Partner/Principal
Integrity & Remediation



David Scott
Managing Director
Crisis & Investigations

Agenda

1. The Current Risk Environment
2. Case Study: Minnesota
3. Fraud, Waste, and Abuse in Local Government Today
4. Cyber Threats to Local Government
5. From Risk to Readiness
6. Key Takeaways for Kentucky

Fraud, Waste, and Abuse in Local Government Today

Recent city and county examples highlight recurring vulnerabilities in local-government operations and oversight.



Access to Public Funds

Ionia Township, Michigan
August 2026

A former township treasurer pleaded guilty after admitting to diverting **\$747,025 in property-tax receipts for personal use** over more than a decade.

ACCESS & RECONCILIATION



Impersonation & Payment Fraud

FBI Nationwide Warning
March 2026

Criminals are impersonating city and county officials and using real permit information to request fraudulent payments.

PAYMENT VERIFICATION



Purchasing Oversight

Cities and Towns Nationwide
2026 Media Coverage

Scrutiny of local-government purchasing-card spending and calls for stronger controls and transparency.

PURCHASING CONTROLS & TRANSPARENCY

Recent events highlight the importance of strong controls over public funds, payments and routine spending.

The Current Risk Environment

Local governments are managing increasingly complex funding amid evolving fraud risks and heightened expectations for accountability.



More complex funding

- Multiple funding sources and requirements
- Reliance on vendors and subrecipients
- Documentation and reporting obligations



Evolving fraud risks

- Vendor and procurement fraud
- Payroll and payment manipulation
- Cyber-enabled payment diversion
- Grant-related misrepresentation



Greater consequences

- Audits and investigations
- Funding interruption or recovery
- Operational and reputational impact
- Loss of public trust

Strong oversight must be proactive, continuous and supported by timely data.

Case Study: Minnesota

Minnesota demonstrates how program-integrity concerns can expand across public programs and become broader funding, oversight and accountability challenges.



Major allegations emerged

Feeding Our Future

Prosecutors alleged approximately **\$250M in false child-nutrition reimbursement claims.**

Federal funding reportedly grew from approximately \$3M to more than \$200M before intervention.

Investigations expanded

Multiple publicly funded programs

Federal authorities executed **22 search warrants** involving childcare, autism services and Medicaid-supported entities.

Subsequent reporting included allegations that warning signs were not acted upon promptly.

Federal action intensified

Funding and provider controls

More than **\$350M in Medicaid payments** were reportedly deferred pending program-integrity reviews.

More than **5,500 high-risk Medicaid providers** were required to revalidate.

Corrective action followed

Oversight and enforcement

More than **3,400 providers were disenrolled**, primarily for incomplete documentation.

Minnesota expanded oversight, enforcement and accountability measures.

Program-integrity concerns can quickly become funding, governance and public-trust challenges.

Cybersecurity is now a local leadership issue

**The practical test is not whether every system is perfectly secure.
It is whether your community can keep operating when something gets through.**

Criminal threats

Ransomware, data extortion, and BEC

Nation-state threats

Water systems, critical infrastructure, Volt Typhoon

Practical fundamentals

30, 60, and 90 day actions

Kentucky in Focus



Ransomware is a continuity crisis

The public judges these incidents by whether services still work.

Ransomware

Systems are encrypted. Services slow down or stop. Recovery becomes a government continuity event.

Data extortion

Attackers steal files first, then threaten to publish resident, employee, or government data.

Business email compromise

A fake invoice, payment change, or urgent leader email can quietly move public funds.



The Record from Recorded Future News

<https://therecord.media/cyberattacks-ransomware-loc...>

Local governments in four states dealing with cyberattacks ...

2 days ago — **Municipalities in California, Oklahoma, Wisconsin and Texas** are all recovering from disruptive cyberattacks that have affected government ...



California City News

Cyberattack Halts Most Government Services in Bay Area Town

The Foster City Council declared a state of emergency Monday night, five days after a cyberattack forced officials to halt most government services.

Mar 24, 2026



TNW TechNewsWorld

Local Governments Face Increasing Cyberattacks

Cyberattacks on local governments are on the rise — and for good reason. "They're target-rich and cyber-poor," explained Michael Klein,...

2 weeks ago



MPR News

Winona County cyberattack is part of a trend as local governments are increasingly targeted

This week's cyber attack on Winona County's government IT networks is part of a trend, as cybercriminals are increasingly targeting local...

Apr 9, 2026



Iran-linked water activity: local infrastructure on the front line

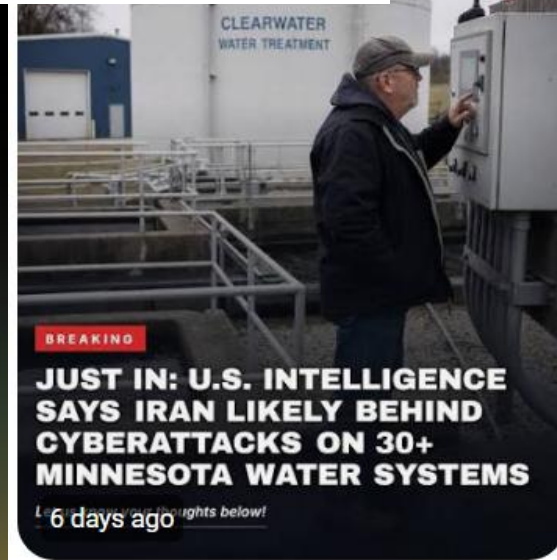
Translate OT risk into pumps, valves, pressure, chemicals, alarms, and public trust.

PRESS RELEASE

CISA, FBI, EPA and U.S. Government Partners Update Warning of Iran-Affiliated Threat Actors Targeting Critical Infrastructure Programmable Logic Controllers

Provides updated actions to detect malicious activity, new observed PLC targeting, and additional mitigations

Released: July 22, 2026



Where's the vulnerability?

PLCs and control systems run physical processes residents rely on every day.

Common error

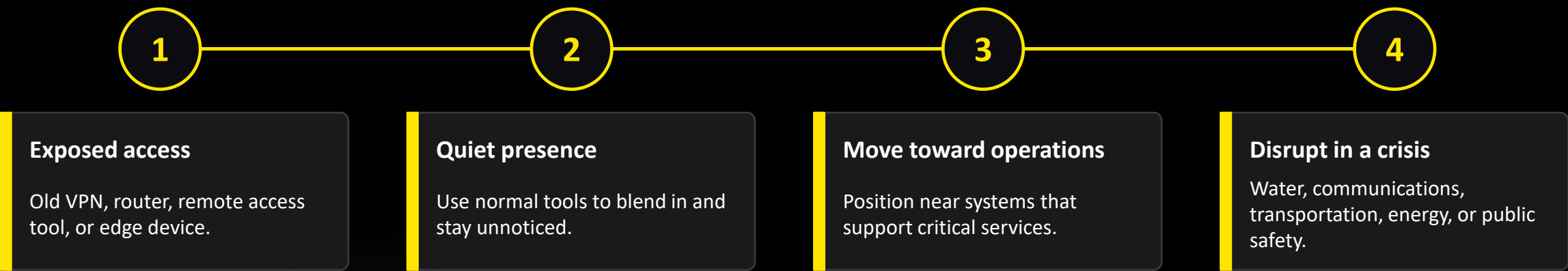
Critical devices are exposed to the internet or still use default credentials.

Questions leaders can ask this week

What equipment is reachable from the internet? Can operators run manually?
Who can change controller settings?

Volt Typhoon: pre-positioning before disruption

Some adversaries are not preparing for a data breach. They are preparing for leverage.



Map what must keep running for 24, 72, and 168 hours. Then practice manual workarounds before an emergency.

Don't get fancy. Get the fundamentals right.

Most serious incidents still exploit common, correctable weaknesses.

First 30 days: know exposure

- Name an executive owner
- List internet-facing systems
- Connect with CISA regional support / MS-ISAC
- Confirm MFA for remote access, admins, email, and finance

First 60 days: close doors

- Patch or replace high-risk systems
- Disable unnecessary remote access
- Remove unused accounts
- Require unique vendor and admin logins
- Segment critical services

First 90 days: practice disruption

- Run ransomware tabletop
- Exercise water, dispatch, or lifeline disruption
- Test restoration from backup
- Prepare public messages
- Brief leaders with a simple dashboard

**The communities that recover fastest are not always the ones with the biggest budgets.
They are the ones that prepared together before the crisis.**

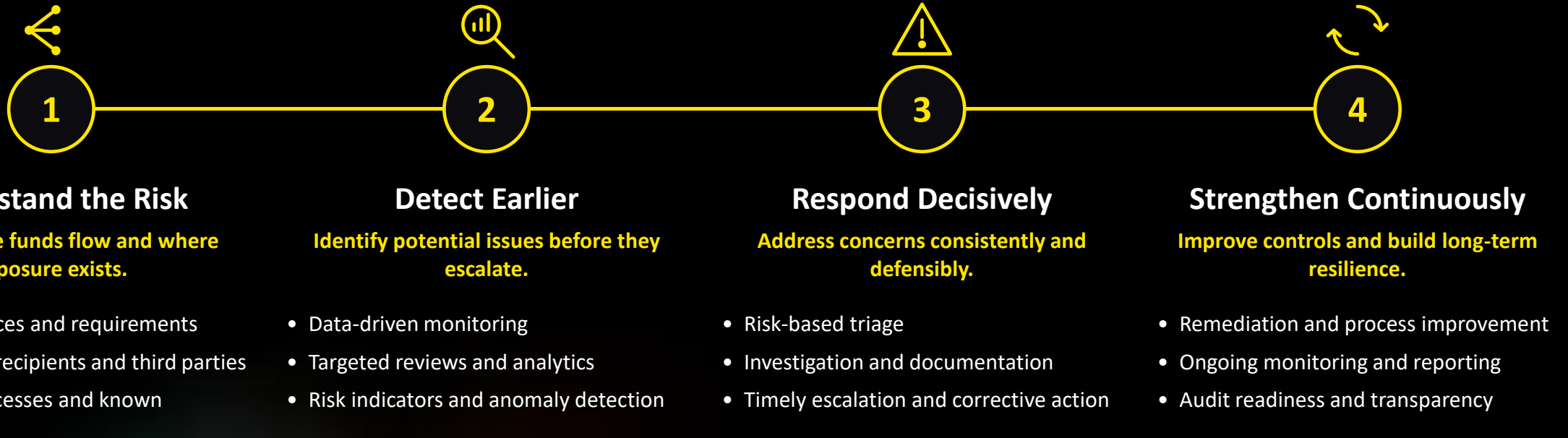
Seven questions every local leader can ask Monday morning

- 1 What services must keep running, no matter what?
- 2 What systems are exposed to the internet?
- 3 Are remote access, email, finance, and admin accounts protected by MFA?
- 4 Can we restore clean backups, and when did we last prove it?
- 5 Can water, dispatch, courts, payroll, and public communications operate manually?
- 6 Who can change critical settings, vendor access, or payment instructions?
- 7 Who do we call before the crisis: state, CISA, FBI, vendors, mutual aid?

Fund the basics. Test the backups. Rehearse the outage. Build relationships before the incident.

From Risk to Readiness

Funding with Confidence helps local governments strengthen oversight, focus resources where risk is highest and demonstrate responsible stewardship of public funds.



The goal is not simply to respond to scrutiny, but to demonstrate responsible stewardship before questions arise.

Key Takeaways for Kentucky Communities

Local governments do not need to eliminate every risk, but they should be able to identify, prioritize and respond to the risks that matter most.



Know How Public Funds Move

Maintain visibility from funding source through final use.

- Understand requirements, restrictions and responsible parties
- Maintain documentation supporting key decisions and expenditures



Focus Oversight Where Risk Is Highest

Apply greater scrutiny where exposure and vulnerability are greatest.

- Prioritize higher-risk processes, transactions and third parties
- Use available data to identify anomalies and emerging patterns



Act When Warning Signs Emerge

Detection creates value only when concerns are assessed and addressed.

- Establish clear ownership and escalation paths
- Document reviews, decisions and corrective actions



Build Readiness Before Scrutiny Arrives

Treat program integrity as an ongoing operating responsibility.

- Test and improve controls before questions arise
- Maintain audit-ready records and communicate transparently

Confidence comes from knowing where funds are going, where risk is concentrated and how concerns will be addressed.