Cybersecurity is the New Public Safety: A "Digital Weather" Guide for Every Town

Winter is coming and you're probably planning to handle the plowing after a blizzard; you wouldn't skip plowing the streets or let it be an afterthought. Yet many communities still treat cyber incidents as one-off IT problems instead of what they really are: public-safety events that can halt 911 dispatch, disrupt water billing, shut down schools, and erode trust.

The "digital climate" is shifting fast, McKinsey article published October 19, 2025 describes how agentic AI is supercharging phishing, deepfakes, and fraud, causing more convincing attacks, operational disruption, and trust erosion. It requires enabling better defenses for cities, towns, and districts, who need a playbook that looks a lot like their storm plan: predict, prepare, drill, respond, and recover.

"The risk is severe, but there are steps that every mayor can take." - CISA, Cybersecurity Toolkit for Mayors

Why now?

Losses are soaring. The FBI's Internet Crime Complaint Center (IC3) logged $16+ billion in reported losses in 2024, up 33% year over year. That's not just businesses; public entities and residents get hit too.

Municipal targets are rising. Independent analyses show government entities faced a substantial increase in ransomware in 2024, with hundreds of public-sector victims across the U.S.

Municipal Operational Technologies (OT) is being targeted: EPA warn of disabling attacks on water systems, U.S. agencies confirm nation-state pre-positioning in critical infrastructure, and CISA has flagged active exploitation of common water-utility PLCs, making legacy control systems a present-day public-safety risk.

Ransomware remains a top pattern. Verizon's 2025 DBIR reports ransomware in roughly 30% of public-sector breaches, underscoring its persistence against agencies and municipalities.

AI is a threat and a tool. McKinsey highlights how AI can both accelerate attacks (deepfakes, automated phishing) and strengthen defense (smarter detection/response). Local leaders must plan for both sides of AI.

Think like emergency management

When a nor'easter hits, every department knows its role. Cyber needs the same muscle memory:

- **Forecast**: watch threat advisories from MS-ISAC/CIS and your state fusion center.
- **Prepare**: harden high-impact systems first (dispatch, water/utility, finance). Use CISA's mayoral toolkit as your checklist.
- **Drill**: run short, realistic tabletops (90 minutes) for ransomware and deepfake/impersonation scenarios.

- **Respond & recover**: practice isolating systems, restoring from backups, and communicating clearly to residents. (Your crisis page and 311 scripts should be pre-approved.)

Proof it works: CIS's Secure Cyber City initiative shows how multi-department collaboration, training, and shared services can measurably improve resilience for small and mid-sized cities.

10 "Buzzfeed-y" moves to weather the next digital storm

1. **Flip on MFA everywhere**
   Email, finance/ERP, remote access, and anything with privileged access. Start with elected officials and department heads, then roll down. (It's the single highest-leverage control.)
2. **Backups you can actually restore**
   Keep at least one offline/immutable copy. Test restores quarterly and record the time to recover your top 5 systems.
3. **Make a cyber phone tree**
   When email is down, who calls whom? Include Mayor/Manager, Police, Fire, DPW, Schools, Finance, IT, and Comms. Print it and put it in go-bags.
4. **Tabletop "Ransomware Tuesday"**
   Usually block 90 minutes. Walk through these stages: detect →isolate →notify →restore →public message. Use CISA's mayor toolkit prompts.
5. **Patch the crown jewels first**
   Prioritize public safety, water/OT interfaces, permitting/records, payroll, and tax systems. Define and track SLAs.
6. **Kill legacy passwords**
   Adopt passkeys or a password manager; block known-compromised passwords. (AI boosted phishing means weak/reused passwords are highly risky.)
7. **Turn on logging + basic monitoring**
   Ensure sign-in, privilege, and configuration logs are enabled and retained for well-defined periods (e.g. ≥90 days). Route critical alerts to a shared "duty phone," and consider AI-assisted detection to help small teams.
8. **Add a one-page "cyber rider" to contracts**
   Require MFA, patch cadence, breach notice within certain period (e.g. 24–72 hours), and proof of backup/restore tests for vendors with town data or network access.
9. **Publish a plain-language outage template**
   Pre-approve web/311/social copy that explains what's affected, what residents should (and shouldn't) do, and where to get updates. (Trust is part of safety.)
10. **Run a deepfake and email phishing drill**
    Finance staff and executive assistants practice the "call-back rule": never act on voice/text/video alone-always verify via a known number. AI makes fake authority incredibly convincing.

Quick Cyber Readiness Checklist

- MFA on email, finance, remote access (staff & elected officials)
- Offline/immutable backups; last restore test date: XXX
- Incident phone tree printed and distributed
- Quarterly tabletop completed (ransomware/business email compromise)
- Patch SLAs (e.g. critical systems ≤14 days; others ≤30 days)
- Log retention (e.g. ≥90 days); notify critical alerts through phone and email
- Vendor cyber rider required on new/renewed contracts
- Public outage message template pre-approved by legal/communications team(s)
- Deepfake/Email Phishing/impersonation policy ("call-back rule") briefed to finance & exec staff
- Join MS-ISAC (free for SLTT) and subscribe to advisories/alerts

The digital climate is changing, treat it like the weather

AI-accelerated threats, rising losses, and ransomware's stubborn grip make cyber a public-safety issue, not just an IT chore. The good news: trusted playbooks exist, and they're sized for small teams and tight budgets. Start with MFA, backups, a phone tree, and a 90-minute tabletop. Then iterate, just like you do after every winter storm.

Acknowledgement & References

1. Cybersecurity in the AI Age, by McKinsey & Company
2. Enhanced Cyber Resilience as a Secure Cyber City, By CISA
3. Municipal Cybersecurity, by Citizens Bank
4. Cybersecurity Toolkit for Mayors, by CISA

