

Guardians of Our Digital Courthouse

- Cybersecurity in Local Government
- Technology Upgrades
- Presented by:
 - Judge/Executive Curtis Dame, McLean County, Kentucky
 - Judge/Executive Adam O'nan, Union County, Kentucky



The New Front Line

- Today's courthouse isn't just brick and stone—it's also servers, networks, and data.
- Every tax record, payroll file, and emergency response plan lives in a digital vault.
- Local governments are prime targets for cyberattacks.
- Even small counties hold valuable data.

The Threat

- **40%** of counties report that the number of attempted, unsuccessful breaches has increased since last year (53% stayed the same, 7% decreased).
- -NACO-Study of Resilience of U.S. Counties

The Threat Landscape

- We're not too small to be a target.
- **Examples:**
 - Ransomware on Kentucky cities and utilities
 - Phishing targeting payroll systems
 - Data breaches causing downtime
- **Risks:**
 - Financial loss
 - Reputation damage
 - Operational paralysis
 - Legal exposure

Common Vulnerabilities

- Outdated software or unsupported systems
- Weak passwords or shared logins
- Lack of staff training
- No off-site backups
- Unsecured Wi-Fi or public access points

A County That Went Dark

- Case Study: A Kentucky county's servers were locked by ransomware.
- Operations halted for 2 weeks. Recovery cost tens of thousands.
- The greatest cost? Lost public trust.

The Role of Leadership

- Cybersecurity starts at the **top**.
- Responsibilities:
 - Make it a standing agenda item
 - Budget for IT defense/upgrades
 - Enforce password policies
 - Partner with KACO, COT, Homeland Security

The Rewards of a Secure System

- Benefits:
 - Builds public trust
 - Ensures operational continuity
 - Lowers insurance premiums
 - Enables safe modernization
-
- “Security isn’t a cost—it’s an investment in uninterrupted service.”

Practical Steps Forward

- 1. Conduct annual cyber audits
- 2. Enforce MFA and strong passwords
- 3. Maintain off-site/cloud backups
- 4. Train staff to recognize scams
- 5. Develop incident response plans
- 6. Work with Ky Homeland Security
- 7. Review cyber insurance coverage

Collaborative Approach

- Cybersecurity requires collaboration:
- All departments—Clerk, Sheriff, EMS, & ETC—share the same risk.
- Protecting county data is a shared responsibility.

Stewardship in the Digital Age

- As public servants, our oath is to safeguard both physical and digital assets.
- Our communities trust us with their information. Let's ensure that trust is never broken.
- “Cybersecurity is 90% leadership and 10% technology—and it begins with us.”

Additional Tech

- GPS Trackers
 - Vehicle Diagnostic, Tracking
- Local Wireless “Intranet” with Point-To-Point.
 - Savings and Dedicated Internet, Reliable and Redundant
- Door Access Control, Fuel Depot Controls, Traffic and Video of Local Property