CYBER SECURITY FOR THE CITIES OF IOWA

Protecting local governments against digital threats

> “This incident underscores a broader truth we need to embrace: Cybersecurity is public safety,” DeWitt said. “Just like police, fire and EMS, protecting our digital infrastructure is about protecting people — their data, their services and their trust in local government.” Natalie DeWitt, president of the Auburn Common Council speaking after the cyber event for St Paul MN

CYBERSECURITY AGENDA OVERVIEW

- Introduction to Cybersecurity for Iowa's City Leaders
- Cybersecurity Basics for Cities
- Risk Landscape for Local Governments
- Building Cyber Resilience
- Tools and Best Practices
- Policy and Governance
- Culture and Communication
- Strategic Next Steps for City Cybersecurity

INTRODUCTION TO CYBERSECURITY FOR IOWA'S CITY LEADERS

IMPORTANCE OF CYBERSECURITY IN MUNICIPAL LEADERSHIP

Protecting Data and Infrastructure-Know what you have so you can protect it

Essential Knowledge for Clerks, Mayors and City Employees- Training and Education and EDUCATION

Clear Action Steps for Protection- Proactive instead of Reactive

CYBERSECURITY BASICS FOR CITIES

DEFINITION AND SIGNIFICANCE OF CYBERSECURITY FOR CITIES

Cybersecurity Overview

Cybersecurity protects city infrastructure and data from cyber threats, ensuring safe and reliable operations.

Common Cyber Threats

Cities face phishing/vishing, ransomware, data breaches, compromised email accounts, and insider threats that jeopardize security and privacy.

Real-World Examples

Midwest municipalities have experienced cybersecurity incidents highlighting the need for robust defenses.

St Paul MN, Des Moines Schools, City Police Departments to name a few

RISK LANDSCAPE FOR LOCAL GOVERNMENTS

SENSITIVE DATA AT RISK: CITIZEN DATA, UTILITY SYSTEMS, FINANCIAL INFORMATION

Types of Sensitive Data

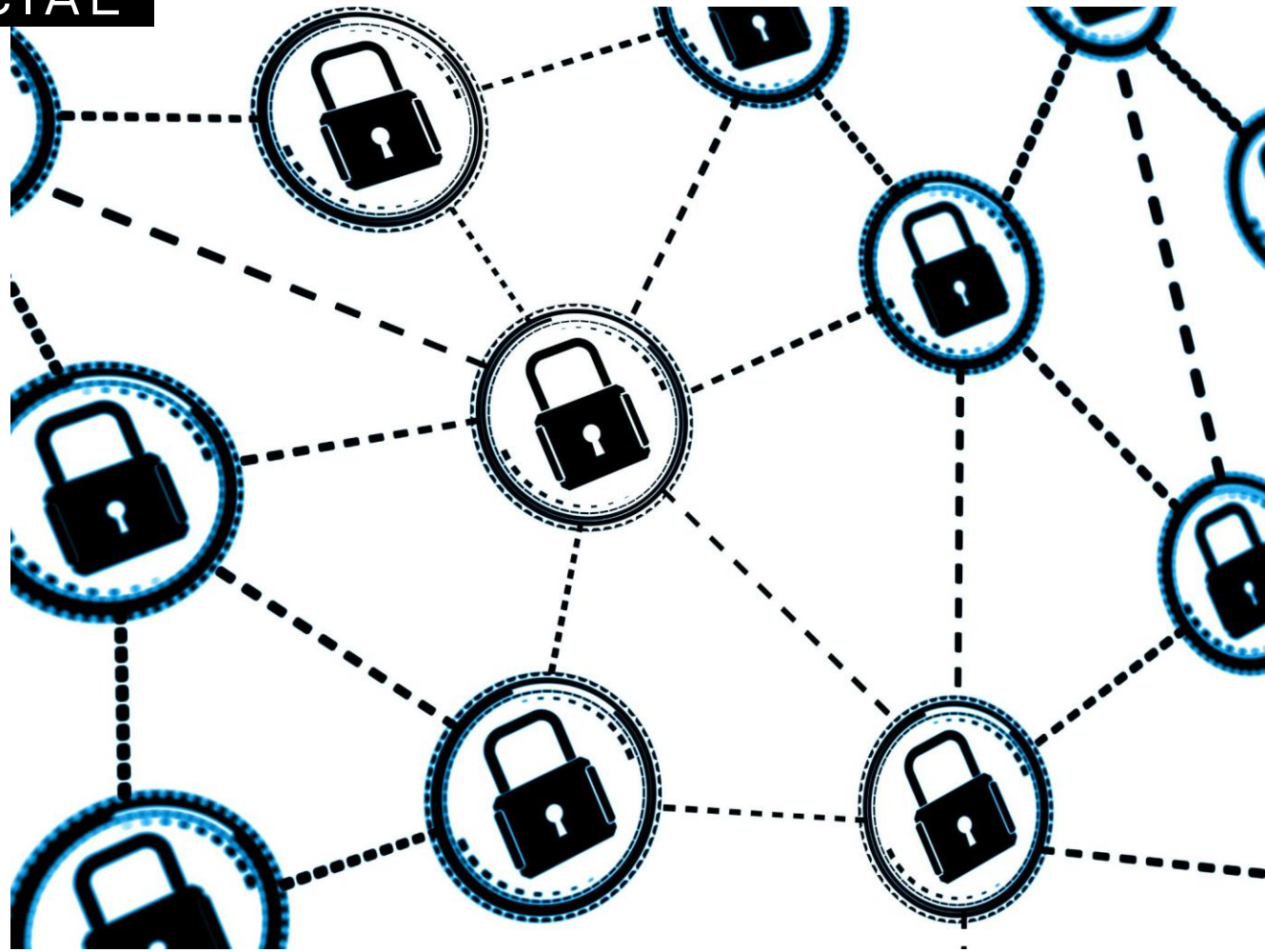
Citizen Data, utility systems, and financial information represent critical sensitive data at risk of cyberattacks.

Targeting Small-town Governments

Small-town governments face increasing cyber threats due to limited resources and vulnerabilities.

Consequences of Cyber Incidents

Cyber incidents can damage reputation, incur fines, and jeopardize public safety in affected communities.



BUILDING CYBER RESILIENCE

CYBER HYGIENE FOR CITY STAFF: PASSWORD PRACTICES, SOFTWARE UPDATES

Password Practices

Strong password creation and regular updates are essential for protecting city systems from unauthorized access.

Software Updates

Timely software updates ensure systems are protected against vulnerabilities and malware attacks.

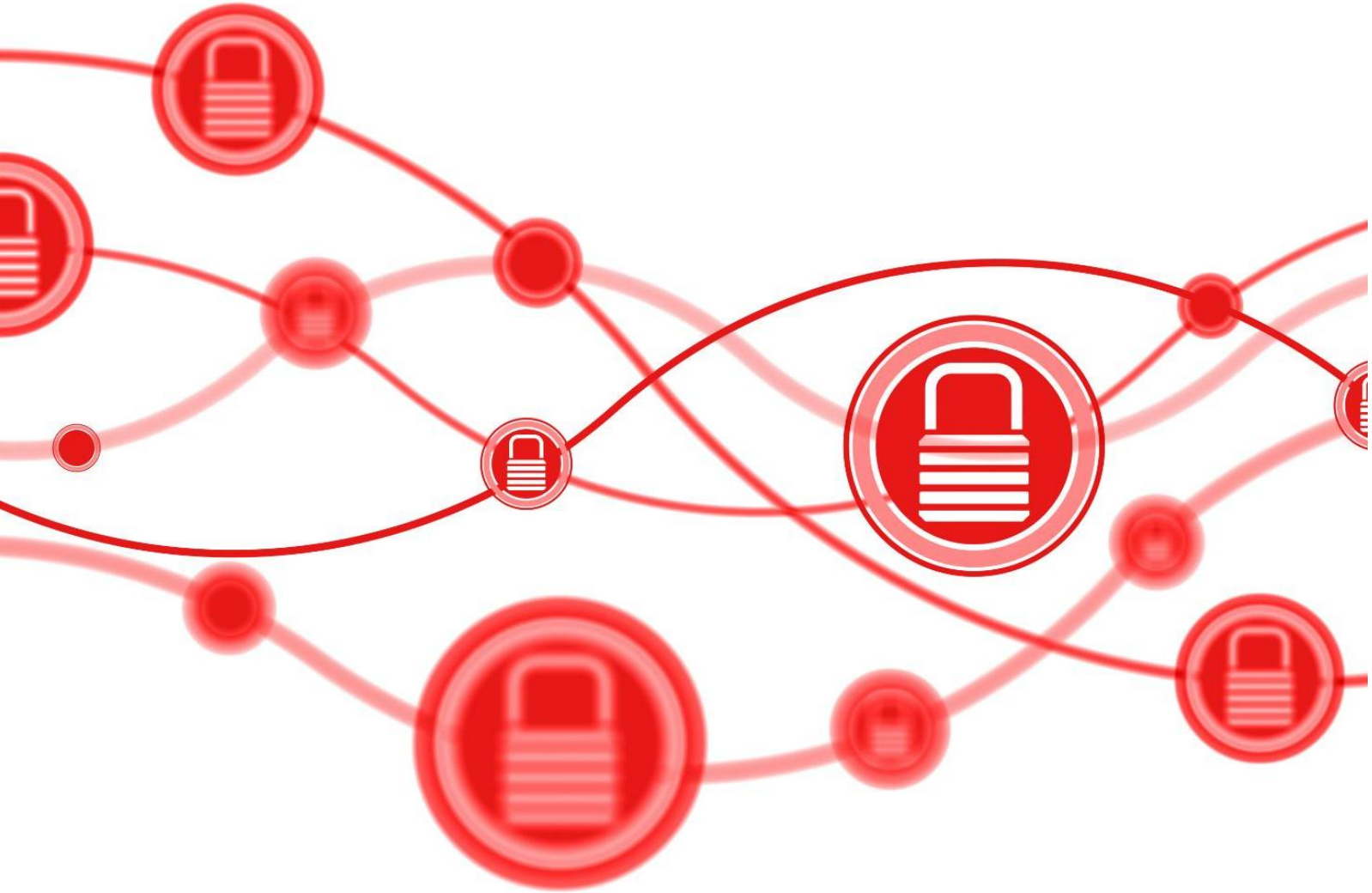
Access Control and Device Security

Role-based access control limits data access, and physical device security prevents unauthorized use.

Vendor Risk Management

Secure procurement and vendor risk management minimize supply chain cyber risks for the city.

TOOLS AND BEST PRACTICES



Multi-factor Authentication

MFA adds security by requiring multiple forms of verification before granting access to systems.

Endpoint Detection & Response- Crowd Strike- 24/7 SOC

EDR tools monitor and respond to threats on endpoints to enhance cybersecurity defenses. Crowd Strike provides free 24/7 protection from the State of Iowa.

Secure Email & Backup

Secure email protocols and data backup protect sensitive information from loss and unauthorized access.- ***Backups are essential for recovering from a cyber event!***

DEVELOPING A CYBERSECURITY POLICY FOR CITY DEPARTMENTS

Cybersecurity Policy Development

Creating comprehensive cybersecurity policies strengthens city departments' defense against cyber threats and data breaches.(CJIS Policies)- *We have multiple templates and examples*

Incident Response Planning

Incident response plans prepare city departments to quickly address and mitigate cyber incidents effectively. *First calls should be to Insurance provider, State of Iowa SOC, FBI. Have a plan before it happens!*

Tabletop Exercises

Conducting tabletop exercises helps teams practice response strategies and improve coordination during cyber incidents. *Work with Local County EMAs and other state and federal resources.*

BUILDING A CYBER-AWARE CULTURE ACROSS CITY DEPARTMENTS

Cyber-aware Culture Development

Fostering a culture of cybersecurity awareness across all city departments improves overall resilience.

Staff Training Initiatives- EDUCATION!!!

Regular training and awareness programs equip staff with necessary skills to identify cyber threats.

Public Communication During Cyber Events

Effective communication strategies keep the public informed during cybersecurity incidents. ***PIO Training!!***

STRATEGIC NEXT STEPS FOR CITY CYBERSECURITY

Building Strategic Partnerships

Collaborate with organizations like Iowa Homeland Security, MS-ISAC, County EMA and Law Enforcement, CISA, ISU, DOM, and ISAC to strengthen cybersecurity efforts.

Cybersecurity Audits and Funding

Conduct thorough cybersecurity audits to identify risks and explore available funding opportunities. ***Work with your insurance providor.***

Digital Resilience Roadmap

Have a plan and have friends!

CYBERSECURITY &
INFRASTRUCTURE
SECURITY AGENCY

Who We Are

The Cybersecurity and Infrastructure Security Agency (CISA) is the Nation's risk advisor, working with partners to defend against today's threats and collaborating to build more secure and resilient infrastructure for the future

IOWA CYBER RESILIENCE CONFERENCE AND WORKSHOP

- **October 16, 2025**
  8:00 am - 4:00 pm

SCHEMAN BUILDING

1805 CENTER DRIVE

AMES, IA 50011

- **Bringing together Iowa's counties, cities, and schools to strengthen cybersecurity, share best practices, and build resilience across the state. All Local Government officials and professionals are encouraged to attend.**

CYBER PROTECTIVE VISIT (CPV)

- Establish and enhances the CISAs relationship with critical infrastructure owners and operators.
- Explains how their facility or service fits into its specific critical infrastructure sector
- Outline the threats to organization and sector to reinforces the need for continued vigilance.
- Provides a tailored overview of the resources available to the to enhance their cybersecurity and resilience.
- Develop an engagement plan for service enrollment, presentations, workshops, assessment, tabletop exercise, Incident Support …

CYBER SERVICES PLANNING - INITIAL

Step One

Cyber Hygiene Vulnerability Scanning (CyHy):

- Maintain enterprise awareness of your internet-accessible systems
- Provide insight into how systems and infrastructure appear to potential attackers
- Drive proactive mitigation of vulnerabilities and reduce risk

Step Two

Cyber Performance Goals (CPGs):

- A set of high-impact security actions for critical infrastructure organizations that address both IT and OT/ICS considerations.
- Mapped to the relevant NIST Cybersecurity Framework subcategories, as well as other frameworks (e.g., IEC 62443).

Step Three

Ongoing Partnership:

- Information sharing
- Assessments
- Tabletop Exercises
- Presentations
- Connection to resources
- Incident Support

Cybersecurity Advisors

Jim Hoflen, Western Iowa
james.hoflen@mail.cisa.dhs.gov 515-707-0332

Shad Roberts, Eastern Iowa
shadrack.roberts@mail.cisa.dhs.gov 563-508-1170

Protective Security Advisors

Chris Judge, Western Iowa
christopher.judge@mail.cisa.dhs.gov 515-901-5571

David Stewart, Eastern Iowa
david.stewart@mail.cisa.dhs.gov 563-676-3419

Emergency Communications Coordinator

Chris Maiers, IA KS MO NE
Christopher.Maiers@mail.cisa.dhs.gov 202-701-3235

Regional Headquarters

CISA.IOD.REGION.R07_Ops@mail.cisa.dhs.gov

CISA Central

SayCISA@cisa.dhs.gov 1-844-Say-CISA

CONCLUSION

Importance of Cybersecurity

Cybersecurity is crucial to safeguard city data and infrastructure from evolving threats and attacks.

Understanding Risks

City leaders must recognize cybersecurity risks to effectively plan and respond to potential threats.

Best Practices Adoption

Implementing cybersecurity best practices strengthens defenses and reduces vulnerabilities in municipal systems.

Security-Conscious Culture

Fostering a culture of security awareness helps communities stay vigilant and resilient against cyber threats.

QUESTIONS AND THANK YOU!!!

Andrew De Haan

ISAC IT Director

Joel Rohne
ISAC IT Strategy Manager
jrohne@iowacounties.org
515-369-7025

Jim Hoflen
Cybersecurity Advisor/Cybersecurity State Coordinator - IA
Cybersecurity and Infrastructure Security Agency
Integrated Operations Division - Region 7 (IA, KS, MO, NE)
515-707-0332
james.hoflen@mail.cisa.dhs.gov

Jordan Hagans
Director of Information Technology – ILOC
Jordanhagans@iowaleague.org
515-974-5351