Cybersecurity for City Administrators

John A. Maschman, JD

LDM
LAMSON DUGAN & MURRAY LLP
ATTORNEYS AT LAW

INTRODUCTION

Why Cities Are Prime Targets

- Limited resources make municipalities vulnerable.
- City infrastructure (utilities, 911) is critical.
- Ransomware groups often target public services.

High-Profile Breach Examples

- Atlanta (2018): Ransomware halted city services.
- Baltimore (2019): Email down for weeks.
- Dallas (2023): Emergency services impacted.

Presentation Objectives

- Understand legal and ethical duties.
- Learn how to avoid breaches.
- Respond confidently if an attack occurs.

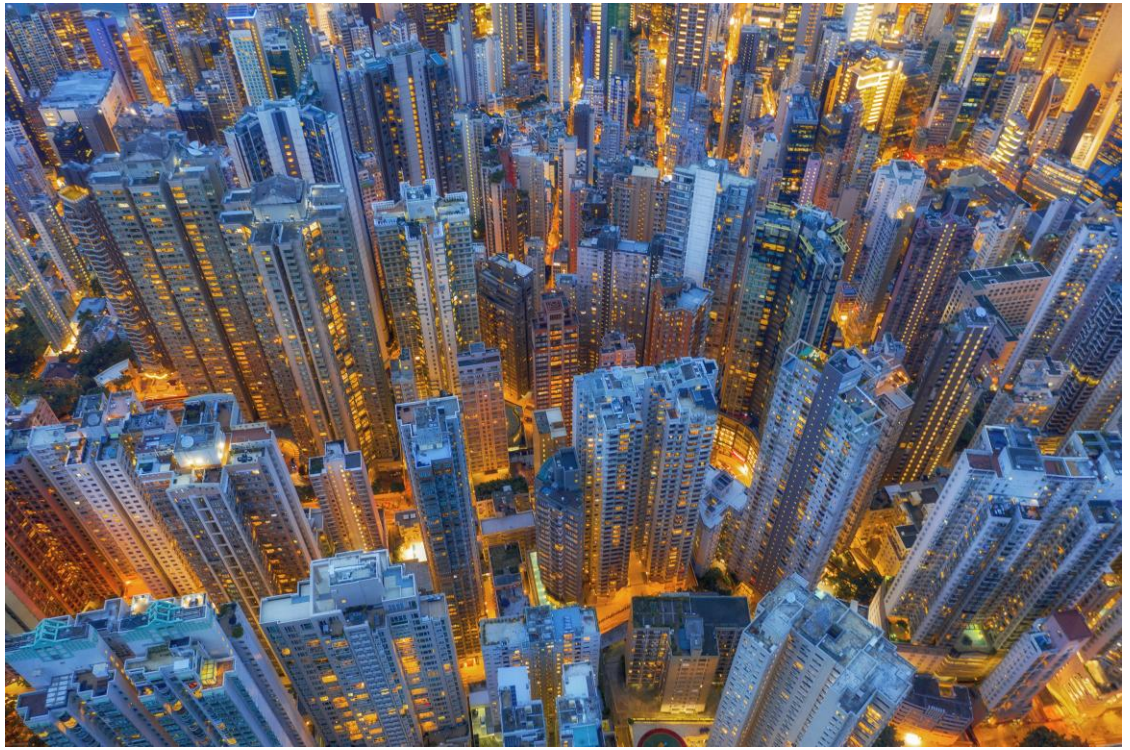
DUTIES TO SAFEGUARD DATA

Role of the City Administrator

- • Set cybersecurity policies and tone.
- • Ensure training and awareness.
- • Champion budgeting for cyber defense.

Legal and Regulatory Requirements

- Iowa Code § 715C – Data breach notification.
- HIPAA – for health data in city services.
- CJIS – for police data; FERPA – if schools included.



Know Your Data

- Create a data inventory.
- Identify sensitive data (PII, financial, health).
- Know where and how it is stored.

PREVENTING BREACHES

Technical Safeguards: Basics

- Use antivirus, firewalls, and endpoint protection.
- Require MFA for email and system access.
- Install software updates and patches promptly.

Technical Safeguards: Advanced

- Encrypt sensitive data at rest and in transit.
- Use secure, offsite backups.
- Segment networks to limit breach spread.

Administrative Safeguards

- Write and distribute an Acceptable Use Policy.
- Enforce role-based access controls.
- Vet and contractually bind vendors for security compliance.

The Human Element: Culture

- Promote a 'see something, say something' culture.
- Provide clear reporting procedures.
- Reinforce good habits with recognition or gamification.

Risk Assessments & Testing

- Conduct annual risk assessments.
- Run penetration testing or tabletop exercises.
- Document results and address gaps.

Cyber Insurance

- Evaluate cyber liability policies.
- Ensure policy covers ransomware and business interruption.
- Understand notification and forensics requirements.

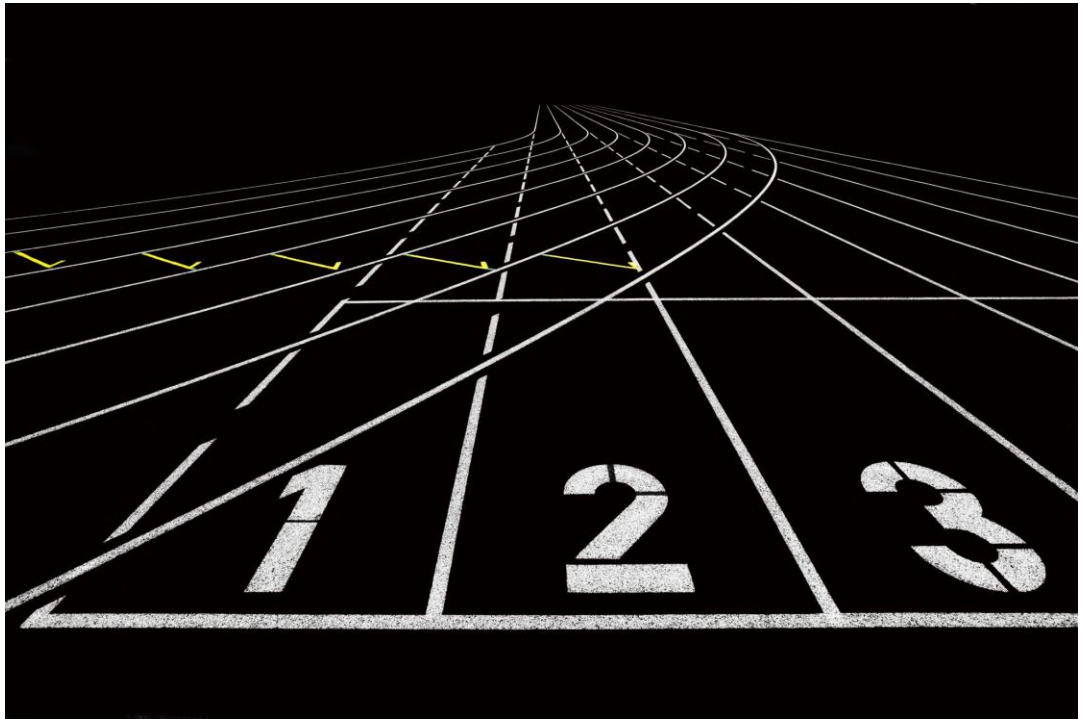
INCIDENT RESPONSE

Signs You May Be Under Attack

- Unusual logins or system slowdowns.
- Locked screens or ransom messages.
- Staff reports of suspicious activity.

Immediate Response Steps

- Isolate affected systems.
- Disconnect from network if necessary.
- Do NOT delete or modify any files.



Preserving Evidence

- Take screenshots of suspicious messages.
- Retain system logs and emails.
- Preserve affected machines for forensic review.

NOTIFICATION AND LEGAL DUTIES

Legal Notification Requirements

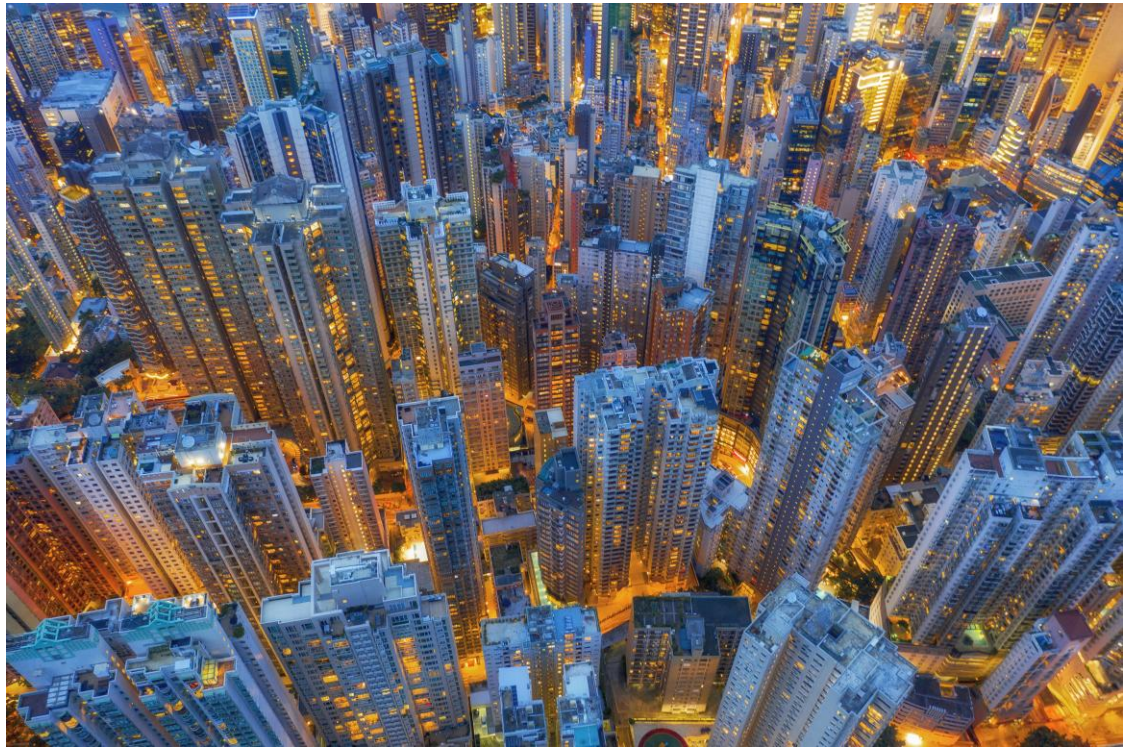
- Iowa Code § 715C requires prompt disclosure.
- Notify affected individuals and AG as needed.
- Public transparency helps preserve trust.

Working with Law Enforcement

- Contact FBI or local cybercrime unit.
- Coordinate investigation and recovery.
- Document all communications.

Coordinating with Insurance

- Follow policy procedures precisely.
- Engage approved forensics and response teams.
- Keep all communication records.



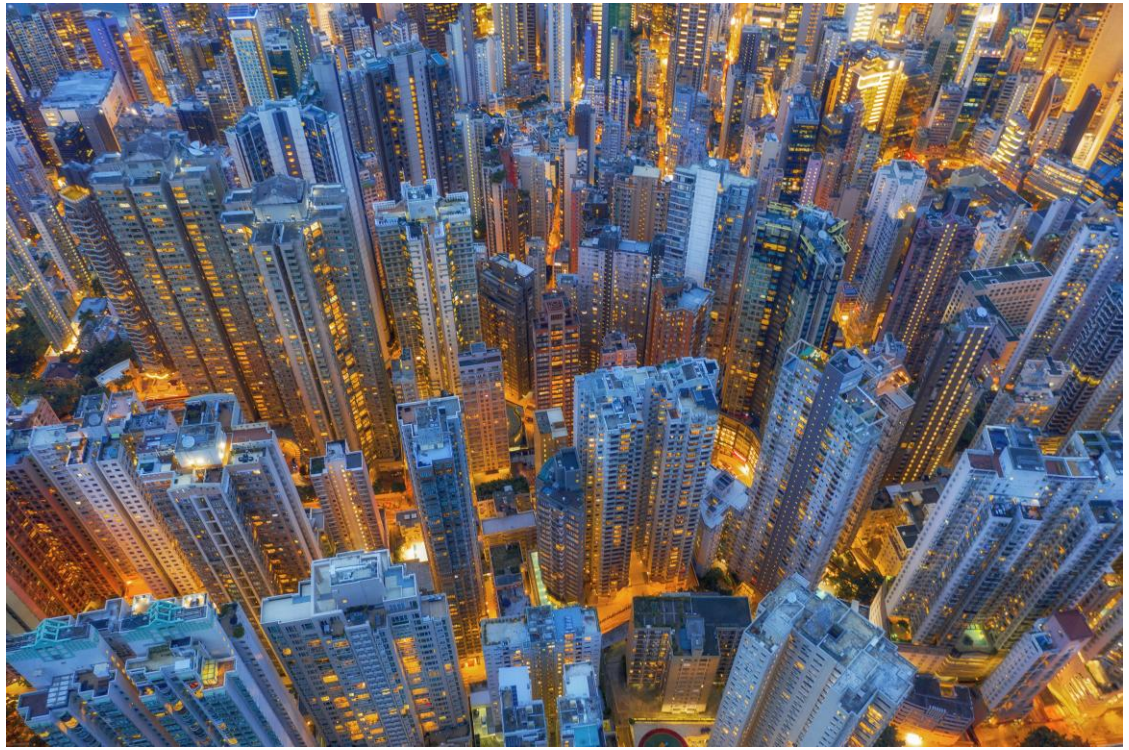
RECOVERY AND LESSONS LEARNED

System Restoration

- Only restore from verified clean backups.
- Patch vulnerabilities before reconnecting systems.
- Monitor systems for signs of residual compromise.

Post-Breach Review

- Conduct internal debrief with all stakeholders.
- Revise response plans based on what went wrong.
- Update policies and training.



RESOURCES AND ACTION PLAN

Federal and State Tools

- CISA.gov cybersecurity guides and alerts.
- MS-ISAC membership for threat sharing.
- Iowa League of Cities cybersecurity resources.

What You Can Do This Month

- Run a phishing test.
- Review and update your Acceptable Use Policy.
- Schedule a tabletop exercise.

Final Thoughts & Q&A

- Every city is a target.
- Preparedness is leadership.
- Your efforts protect public trust.

Thank you!

JOHN A. MASCHMAN
ASSOCIATE ATTORNEY

jmaschman@ldmlaw.com

515.513.5003

LDM
LAMSON DUGAN & MURRAY LLP
ATTORNEYS AT LAW