Protecting Public Funds: Cybersecurity Best Practices for Finance Leaders

- Presented by Jonathan Strong
- Senior Account Executive, VC3

- GFOAT Conference 2025

Introduction

Municipalities a Big Cyber Target

In 2020 **44%** of cyberattacks targeted **municipalities.**

More than **70%** of ransomware attacks target **local** government.

Nation states like to **target municipalities.**

90% of successful cyberattacks start **in email.**

More than **70%** of phishing attacks against government orgs go after **login credentials.**

Only **38%** of state/local government employees trained about ways to **prevent ransomware**.

97% of municipal officials use email to share sensitive documents.

The average time to identify a breach is over **200 days**

The Cyber Threat Landscape

- 78% of ransomware attacks in municipalities target financial systems.
- Dallas (2023): Ransomware shut down police and financial systems.
- Atlanta (2018): $17M in recovery costs after attack on city systems.
- Threats include phishing, vendor compromise, and ransomware.
- Public trust and budget integrity are at risk.

Cybersecurity Essentials for Finance Teams

- Multi-Factor Authentication (MFA) on all systems.
- Strong password policies and access controls.
- Regular data backups—tested and verified.
- Employee training to recognize phishing attempts.
- Secure configurations for accounting software.

Microsoft:

99.9%

of account
compromise attacks
can be blocked by MFA

Arete:

94%

of ransomware
victims investigated
did not use MFA

Sources: https://www.microsoft.com/security/blog/2019/08/20/one-simple-action-you-can-take-to-prevent-99-9-percent-of-account-attacks/

Governance and Cyber Budgeting

- Ensure cybersecurity is included in annual budgets.
- Review and update cyber liability insurance policies.
- Conduct risk assessments and policy reviews annually.
- Evaluate third-party vendors' cyber hygiene.
- Ensure city-wide incident response plans are up to date.

What’s at Stake Financially

- Downtime costs: lost revenue, overtime pay, penalties.
- Legal and consulting fees for breach response.
- Cyber insurance deductibles and policy gaps.
- Reputational damage and public trust loss.
- Budget diversion from other services to cyber recovery.

How VC3 Helps Municipalities

- End-to-end cybersecurity solutions for local government.
- 24/7 threat monitoring and incident response.
- Backup & disaster recovery for critical systems.
- Compliance support with federal and state regulations.
- Tailored cybersecurity plans based on your risk profile.

Q&A and Next Steps