Local Government and the Cybersecurity Crisis

Prepared for:
Association of Local Government Auditors’ (ALGA) Regional Training Conference
Who Am I?

Quote for the Day:
There is no reason why good cannot triumph as often as evil. The triumph of anything is a matter of organization. If there are such things as angels, I hope that they are organized along the lines of the Mafia.

~ Kurt Vonnegut, The Sirens of Titan

Sarah Rees
Director, Cyber Workforce Academy

Superpowers include:
Out-of-the-Box thinking, Scuba diving, Meme Appreciation, Cats
Cybersecurity Crisis

crisis - /ˈkrɪsɪs/ - noun

- a time of intense difficulty, trouble, or danger.
- a time when a difficult or important decision must be made.

~ Oxford Dictionary
How do we Secure our Assets

- Principles are same for Government/Private Industry
- Is it harder for Government?
  - Fewer resources/skilled people
  - Multiple complex standards and regulations
  - Policy vs. Practice
Why is Cybersecurity Hard?

Diagram showing layers of cheese with labels: People, Process, Technology, Hazard leading to Loss.
Threats to Local Government

Threats to local government are similar to those that span other sectors. However, the wide array of responsibilities & information at play present a much larger attack surface.

- Ransomware
- Phishing
- Insider Threats
- Inadvertent Errors
ATLANTA
est. population - 486,000

Ransom Demand: $51,000

- Recovery Estimates ~ $9.5 million
- 6 million citizens impacted
- Targeted hospitals, gov. offices (city/municipal)

2018
City Ransomware Attack
LEEDS
est. population: 12,000

2018
City Ransomware Attack

Ransom Demand: $12,000
- Negotiated and paid $8,000 in ransom
- Most files restored (not all)
- Low ransom demand means payment is a more affordable option for many
Port Orchard, WA

- Strongest Tornado in WA since 1986
- Wind speeds of 120-130 mph

Dec 2018 Tornado
Tornadoes & Tunnel Vision

Tunnel vision approach to trends may leave us unprepared.

Disaster preparedness should be holistic.

 Cybersecurity preparedness should be holistic.

Today's trending malware does not always predict tomorrow's catastrophic cyber attack.
Measuring Preparedness

Start with Compliance

...SO MANY STANDARDS...

- PCI DSS, HIPAA, FERPA, FISMA, NIST 800, GDPR, GBLA (to name a few)

- EO 13636 (Improving Critical Infrastructure Cybersecurity) led to NIST Cyber Security Framework (CSF)

- Crosswalks and Mapping (many already exist!)
**Example:**

<table>
<thead>
<tr>
<th>Function</th>
<th>Category</th>
<th>Subcategory</th>
<th>Relevant Control Mappings²</th>
</tr>
</thead>
</table>
| **ID.AM-1:** Physical devices and systems within the organization are inventoried | **Asset Management (ID.AM):** The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the organization’s risk strategy. | • CCS CSC 1  
• COBIT 5 BA09.01, BA109.02  
• ISA 62443-2-1:2009 4.2.3.4  
• ISA 62443-3-3:2013 SR 7.8  
• ISO/IEC 27001:2013 A.8.1.1, A.8.1.2  
• NIST SP 800-53 Rev. 4 CM-8  
• HIPAA Security Rule 45 C.F.R. §§ 164.308(a)(1)(i)(ii), 164.310(a)(2)(ii), 164.310(d) |
| **ID.AM-2:** Software platforms and applications within the organization are inventoried | | • CCS CSC 2  
• COBIT 5 BA09.01, BA109.02, BA109.05  
• ISA 62443-2-1:2009 4.2.3.4  
• ISA 62443-3-3:2013 SR 7.8  
• ISO/IEC 27001:2013 A.8.1.1, A.8.1.2  
• NIST SP 800-53 Rev. 4 CM-8  
| **ID.AM-3:** Organizational communication and data flows are mapped | | • CCS CSC 1  
• COBIT 5 DSS05.02  
• ISA 62443-2-1:2009 4.2.3.4  
• ISO/IEC 27001:2013 A.13.2.1  
• NIST SP 800-53 Rev. 4 AC-4, CA-3, CA-9, PL-8  
• HIPAA Security Rule 45 C.F.R. §§ 164.308(a)(1)(ii)(A), 164.308(a)(3)(ii)(A), 164.308(a)(8), 164.310(d) |

NIST Security Control Mappings to Corresponding HIPAA Security Rules

Available at hhs.gov
U.S. Dept. of Health and Human Services
Cautionary Tales

- Examining cases of failures
- Aligned to NIST Categories
- Details, company/individual(s) names are redacted
Company "A"

EPIC FAIL
Seriously...How does one manage that?

Identify-Asset Mgmt (ID.AM)
- Multiple, separately maintained inventory lists
- Leadership/processes relied on employees to "know" their systems
Company "A" HACKED

- Critical patches missed on assets that were not properly identified

“At the time that the breach was announced, I wasn’t even aware that we were running XXX [software] in the particular environment.”

~ Senior VP & CIO of Impacted System

Install updates
Company "B"

Identify-Governance (ID.GV)
Respond-Analysis (RS.AN)

- Poor leadership/reporting structure
- Key Executives (limited skill/awareness)
- Limited ability investigate incidents
Company "B" INCIDENT RESPONSE

Incident Timeline = 70+ Days

Incident Analysis

- Logging of the [impacted] servers only retained for 14 days (30 days online)

Governance

- CIO/CISO in separate departments
- CISO reported to CLO (Legal)
- Limited understanding/involvement
Company "C"

Protect-Access Control (ID.AM)
Protect-Data Security (ID.DS)

- System Credentials not secured
- Sensitive Data not Encrypted
- No File Integrity mechanisms in place
Company "C" DATA BREACH

- Attackers ran 9,000 queries against multiple, unrelated databases

- 265 queries returned un-encrypted PII

- Lack of file integrity software allowed attackers to add files to system to enable remote access
WHAT IF I TOLD YOU

ALL 3 OF THESE EXAMPLES ARE THE SAME COMPANY?
Equifax Breach, 2017

- Global Company
- $3.36 billion in revenue (2017)
- Over 145 million American Citizens data compromised
Investigation and Findings

- U.S. House of Representatives Committee on Oversight and Government Reform

- Report released 10 December 2018

- Most glaring conclusion:

" Entirely Preventable "
Crisis Response

- No Magic Bullet
- No One-Size-Fits-All Approach

Cybersecurity is not just about money; it's about the potential for interference in systems that keep our society functioning
Organizational Success

An audit is just a snapshot in time. Cybersecurity must be continuous.

Organizations must be:
- honest with themselves and others
- willing + able to learn & improve