IT Security in Local Government

Michael Hamilton
Key Takeaways

• Government is a target
• Local government is least-protected
• Possible impacts include records breach, theft of funds, and disruption of critical services
• Reasons for lack of attention to the issue
Bad Outcomes – Quick Inventory

• Loss of protected records
• Electronic theft (funds, or intellectual property, for the private sector)
• Service infrastructure disruption
• BONUS PAIN: regulatory scrutiny, fines, bond rating
**Recent Public Sector Events**

**Montgomery County Public Schools Says It Was Target of Cyberattack**

Electronic disruption lasted three days, district spokesman says

**Man Behind 911 Call System 2016 Cyberattack Sentenced to Probation**

Meetkumar Desai pleaded guilty in August to felony count of solicitation to commit computer tampering

**Cyber-criminals attack Atlanta, Fulton, and Clayton school districts, paychecks stolen**

*Posted: Oct 03, 2017 9:54 PM PST*
*Updated: Oct 04, 2017 8:04 PM PST*

October 05, 2017

**City of Englewood, Colo. hit with ransomware**

The attack left the city's civic center unable to process credit cards and the city's library unable to place items on hold or accept late fines, according to an Oct. 4 press release.
Law Enforcement evidence held for ransom, utilities taken offline and transportation derailed. All have happened in the last 12 months. Sometimes it feels like TV supervillains from our childhood have come to life; CHAOS, Cobra and, worst of all, the dreaded Legion of Doom. But in a world of international terror organizations and state-run subversive groups, such supervillains would likely do less damage.
Traffic Management
Water Purification
Waste Treatment

Wastewater Treatment

Internal Pump Station & Grate
Sand Trap
Preliminary Sedimentation
Transition Pump Station
Air- and Denitrification Tank
Final Sedimentation
Return Sludge Pump Station
Blower

Gas Container
Gas Engine / Generator
Boiler
Heat

Preliminary Drain
Heat Exchanger
Sludge Storage
Sludge Press

Pump Station
Motor Control

CRITICAL INFORMATICS
Communication for Law Enforcement and Public Safety
Next-Generation 9-1-1
Emergency Management
Energy Generation, Distribution
Automated Metering

How Automated Meter Reading Works

- **Meter**: An electronic high tech meter installed at a location uses accurate and secure radio frequencies.
- **Wireless Service Network**: The data is transmitted wirelessly.
- **Billing System**: Meter data is collected and used to generate your monthly bill.

CRITICAL INFORMATICS
<table>
<thead>
<tr>
<th>CoS Incidents</th>
</tr>
</thead>
<tbody>
<tr>
<td>HVAC systems compromised</td>
</tr>
<tr>
<td>Power Marketers targeted</td>
</tr>
<tr>
<td>Deeply compromised energy utility infrastructure</td>
</tr>
<tr>
<td>Denial of service attacks</td>
</tr>
<tr>
<td>Vulnerable transportation management</td>
</tr>
<tr>
<td>Telephony equipment compromised</td>
</tr>
</tbody>
</table>
What Got Us Here?

• Management by Landmine
• Thin budgets and poor value proposition
• No access to qualified practitioners
• Technology moves faster than policy
• But more than anything – MISPLACED FOCUS
Can We Dig Out With Legislation?

Amid growing threats, Iowa lawmakers push for better state and local cybersecurity

Lawmakers unveil bill to help state, local governments with cybersecurity

Bill would launch cybersecurity grant program for state and local governments
Thanks for Listening!

Michael Hamilton
Critical Informatics
Michael.Hamilton@CriticalInformatics.com
@critinformatics
@seattlemkh

IT Security News Blast:
https://criticalinformatics.com/it-security-news/