Top Five Things You Need to Know About Cybersecurity

Larry Mattox, VC3

Session #7
Cyber breaches are more sophisticated and can happen to any size organization.
Victims of Cyber-espionage

- CNN, Washington Post, Time Magazine, Adobe, Target

- 70 small, mostly rural, police and sheriff offices
  - Targeted by company they investigated. Hacked into computer systems, defaced websites and exposed sensitive information (emails, tips on suspected crimes and profiles of gang members).

- Texas County
  - $200,000 theft of electronic fund transfers for schools and cities.

- Australian City
  - Computer expert rejected for city job hacked into wastewater management system.

Source: National Security Cyberspace Institute, National League of Cities, Agio
Top 5 Things You Need to Know

1. Time is of the essence
2. Why municipalities are vulnerable
3. How cyber attacks happen
4. How they penetrate your municipal world
5. How to limit risk
1. Time is of the Essence

- 84% of breaches required minutes to execute
- 66% took more than a month to be discovered
- 22% took greater than a month to contain the breach, alleviate the problem, and recover
As the Clock Ticks, Critical Questions Exist

- Has the problem stopped, or is it continuing?
- What is the scope of any damage?
- Who will you call to help?
- What other offices or partners must you notify?
- Can you determine if data breach was malicious or an accidental loss?
- What are your municipality’s legal requirements for notification of impacted individuals?
2. Why Municipalities Are Vulnerable

One employee opens email attachment with a virus, the town’s entire system is be affected.

- Think they are low profile targets... “nothing to protect since information is considered public.”
- Cannot afford IT staff to oversee data protection 24x7.
- Therefore... less emphasis on prevention and protection.
- Increasingly running critical services on computers – easily penetrated by cybercriminals or disgruntled employee.
2. Why Municipalities Are Vulnerable (cont.)

- Confidential/sensitive information stored about citizens
  - Personal and financial information
  - Employee benefit and retirement information
  - Tax records
  - Court and criminal records

Makes government a high-value target for a cyber-attack/data breach…
3. How Cyber Attacks Happen

92% of incidents analyzed fit into 9 basic patterns:

1. Miscellaneous errors
2. Crimeware
3. Insider and privilege misuse
4. Physical theft and loss
5. Web app attacks
6. Denial-of-service attacks
7. Cyber-espionage
8. Point-of-sale intrusions
9. Payment card skimmers

*From 2014 Data Breach Investigations Report
4. Top Ways They Penetrate Your Municipal World

98% of attacks fall into 4 categories:

1. Errors (34%)
   - Posting private data to public site accidentally
   - Sending information to wrong recipients
   - Failing to dispose of documents or assets securely

2. Insider misuse (24%)
   - Non-work-related Internet surfing
   - Use/abuse of personal email or instant messaging
   - Downloading music or pirated software
   - Unauthorized copying of files to portable storage devices (i.e. USB drive)

3. Crimeware (21%) (Identity theft via social engineering or technical stealth)
   - Takes funds from online accounts or completes unauthorized transactions

4. Lost/stolen assets (19%)
5. How to Limit Risk

- **Policies**
  - Documented rules for various situations

- **Training**
  - Might vary by department, but must be done

- **Technical Controls**
  - Having the right technology and relationships in place
Policies and Training Can Limit Your Risk

- Be cautious about opening attachments or downloading files from emails
- Don’t click on, or reply to, email or pop-up messages that ask for personal or financial information
- Don’t email personal or financial information
- Review credit card and bank account statements as soon as you receive them
- Have qualified IT support, with security experience
- Continue training and ongoing awareness
Technology Can Protect Your City

- Have IT support that is well-versed in cyber-security
- Anti-virus, anti-spyware, monitoring, patching, etc. are *fundamental* methods to protect against threats from the outside
- Encrypt data and utilize authentication process
- Understand current software programs and restrict account access
- Cloud technology brings enterprise class services, and expertise, to your city
- Test incident response capabilities and plan
- Review annually
Homework

• Share this information with your key staff
• Confirm policies are in place to address these concerns
  • If no, make it a priority to create policies
• Since Cybersecurity breaches are a “disaster”... find out if your municipality has a viable **Disaster Recovery solution**
  • Find out if your municipality has a written **Business Continuity** plan