Municipal data is under attack every day. In fact, cybersecurity is the top concern for local government IT officials. Take the right steps for protecting data by learning how to secure it and how to respond if a breach does occur.
Prize Drawing

Amazon Echo

Apple Watch
Protecting City Data

Larry Mattox, VC3

Session #8
How a 7-year-old girl hacked a public Wi-Fi network in 10 minutes

Cybercrime is child’s play, it seems, as seven-year-old Betsy Davies succeeds in hacking a Wi-Fi hotspot

Betsy used easy-to-find online tutorials to access devices over a public Wi-Fi connection

Related topics
Data
Data breach
Security

Related articles
Do you know more about cyber security than David Cameron? Take the quiz
The future of cybercrime

Security Challenges Continue to Grow

Security breaches getting more sophisticated, threats more complex and can happen to any size organization
The Security Challenge

• Topic can be overwhelming
• Concepts are confusing
• Seen as purely an IT issue
• Ignore until an event occurs
Time is of the Essence

- 84% of breaches required minutes to execute
- 66% of those took more than a month to be discovered
- 22% took greater than a month to contain the breach, alleviate the problem and recover
How Your World Is Breached…

In the Public Sector 98% of attacks fall into 4 categories:

- Errors (34%)-
  - Mistakes that compromise security

- Insider misuse (24%)-
  - Non-work related, while on the job

- Crimeware/Outsiders (21%)-
  - Theft via social engineering or technical stealth

- Lost/stolen assets (19%)
Sound Policies Create Awareness

“Education is the first line of defense”

• Explain the ramifications of a data breach
• Start with basics (simple as password policies, opening of emails, etc)
• Document rules for various situations
Technology Can Protect Your Data

- Assure your IT support is well-versed in cyber-security
- Have strong, pro-active security in place
  - Anti-virus, anti-spyware, monitoring, patching, etc. are fundamental methods to protect against threats.
  - Strong encryptions and solid authentication process
- Have a solid data backup and disaster recovery plan
- Cloud technology brings enterprise class services, and expertise, to your organization
Key Components for a Good Security Plan

Having a security expert can be invaluable

- Have a security audit
- Develop a plan
- Educate your team
- Protect your network and Internet
- Protect against viruses, spyware and spam
- Review your security, and your plan, regularly
How to Respond to a Security Breach

It is your responsibility, so be prepared

- The response process has many steps.
- It is city’s responsibility to respond (or have a professional respond) and provide immediate detailed information.
- So, know the state’s breach notification law.
- Have an incident response team.
- Act quickly, but use caution about communicating too much information too quickly.
- Make sure sufficient facts have been gathered.
Train, Test and Plan

• Training
  • Educate employees on security threats
  • Train them to recognize and respond
  • Continue, and upgrade, your training

• Testing
  • Test protocols and procedures
  • Engage third party in tests and evaluations

• Pre-planning and identifying
  • Municipalities and partners working together to develop plans for response to security threats.

What's the plan?
What’s Next?

- Share this information with your key staff
- Are policies in place to address these concerns?
- If no, make it a priority to create policies
- Security breach is a “disaster”... so find out if your municipality has a viable Disaster Recovery solution
Prize Drawing

Amazon Echo

Apple Watch