LEO S. LUTZ
Mayor

EVAN M. GABEL
Solicitor

HEATHER ZINK
Borough Council President

MARK E. STIVERS
Borough Manager

Presentation for the Joint Public Hearing
of the Senate Local Government Committee
and Senate Communications & Technology Committee

Wednesday, January 31, 2024, 1:00 pm to 3:00 pm

Presented by: Mark E. Stivers, AICP, Borough Manager for the Borough of Columbia representing the Pennsylvania State Association of Boroughs (PSAB)

Subject: Cybersecurity Issues for Local Governments and Municipal Authorities

As local governments work to meet the needs of their citizens, safety and security are always foremost in the minds of local officials.

Many of us now have security barriers in our lobbies and have or are installing bulletproof glass in our lobbies to protect our staff.

The Borough of Columbia has recently expanded the security cameras in our office and last year installed "panic buttons" in our Council chambers. Our Code Compliance officers often need to take a police officer with them when inspecting properties.

A newer area of safety and security has emerged in the digital age: the need for Cyber Security.

The Borough of Columbia is a larger Borough compared to many across the Commonwealth. We have a population of just over 10,400 residents and an annual general fund budget of just over $8 million. We have 7 council members and a Mayor, and over 30 volunteer positions that serve on our boards and committees.

And like many, we are looking for new ways to improve the level of service we can provide our citizens. So many of us like to grab our smartphone to pay a bill. Scan a QR code to pay for dinner. The Borough implemented Park Mobile to allow people to pay for parking via a phone app.

But what about paying for rental registration, parking tickets, code compliance fines? Can that be done online? How can our stand holders at the Columbia Market House pay their monthly rent online?

In order for municipalities to move into the digital age, we must be able to secure sensitive information from hackers.

Enter the need for Cyber Security:

- The Borough operates under a general fund budget of about $8.6 Million. That covers a full-time police department, Borough staff, and several recreation facilities.
- We have about 50 full and part-time staff members, 7 Borough Council members and about 30 volunteers on our boards and committees.
- In 2021, Columbia paid just over $40,000 for new servers and new firewalls.
- We spend about $80,000 a year for IT service.
- We spend about $15,000 a year to upgrade computers.
- We spend about $11,000 a year on cell phones for key staff members.
- We spend just over $9,000 a year on cyber security insurance that provides us with $1 Million in aggregate coverage that includes:
    - Security Breach
    - Data restoration
    - Public Relations expenses
    - Extortion and ransom payments
    - Fines and Penalties
- Need for highspeed broadband connections to allow data backups to be securely transferred to an off-site location.

Key points for Local Municipalities:

- Cyber Security is an ongoing issue and constantly moving target. Like code enforcement, we are never done!
- First and foremost is training staff and officials. Our IT company will send out “fake” emails to test staff members’ ability to spot dangerous emails.
- Keeping equipment and security protocols up to date.
- Maintain and verify data back ups and have a procedure for data restoration.
- Getting more information stored electronically (digital document conversion, management and storage
- Establishing security policies and procedures and keeping them up to date.
- Communication with residents is also critical. We use our website, social media (Facebook and linked in), newsletter, public meetings, and TextMyGov.
- Regularly test vulnerabilities and weaknesses

MFA (Multi-Factor Authentication):

- MFA is a critical tool that municipalities can use to protect against attacks.
- MFA requires a user to enter an additional information such as a security code or confirmation via their smartphone, computer, or from a phone call.

- MFA needs to be used on all business-critical systems, e.g., email, bank accounts, secure medical information.

Currently there are three main methods of MFA:

1. Knowledge based – This is information that is generally only known by the person. Examples include mother's maiden name, first pet, favorite movie or song. In the age of information, this method is becoming less secure.
2. Possession based – This is based on things that you have such as bank security fob, a USB key, receiving a one-time code on your cell phone.
3. Inherence-Based or Biometric security. These are things that are unique to each person. This will include fingerprints, voice recognition, and facial recognition (used on many cell phones now),

Issues with MFA that impact Municipalities:

- Issue – Not all staff have Borough-issued cell phones.
- We have union staff that don't want to use personal devices for work related activities.
- Costs to install an external fingerprint scanner on every computer.
- Microsoft Windows HELLO – Need to migrate all computers to Windows 11.

Case study:

Rivera Beach Florida. Someone in the police department clicked on a link in an email. The result was a ransomware attack that shut down the entire city. It cost the city approximately $600,000 to get their system released and another $941,000 in new equipment.

Conclusion:

Cyber Security is mission critical for municipalities, but the costs may exceed the ability of some municipalities to fully implement these protocols. Phishing attacks using AI technology is only getting more advances and more difficult to catch. Significant investment is needed to get municipalities secure and protected from cyber attacks.