CYBER SECURITY CONCERNS FOR MUNICIPALITIES
PANELISTS INTRODUCTIONS

- Tasha Jackson
- Nick Ippolito
- Chris Washington
CYBER SECURITY: A 3 PART DEFINITION

- Protecting information and systems from major threats
  - Cyber terrorism - disruptive use technology by terrorist groups to further their ideological or political agenda
  - Cyber warfare - nation-states using information technology to penetrate another nation’s networks to cause damage or disruption.
  - Cyber espionage - to obtain secret information without permission from its owners to gain strategic, economic, political, or military advantage
THE ACTORS!

- Hacker who finds security vulnerabilities and discloses it to the developer
- Criminals performing illegal activities for personal gain and attacking others
- Attempts to compromise an organization without permission and allows them to fix the problem.
THE THREAT

- External
- Internal
1. **Reconnaissance:** Attackers carefully plan their attacks. Research, identify, and select targets.

2. **Weaponization & Delivery:** Craft deliverables to catch specific interests (Cats!)

3. **Exploitation:** Once “inside” an organization, they can activate attack code to ultimately take control of the target.

4. **Installation:** Attackers will seek to establish privileged operations, root kit, escalate privileges, and establish persistence.

5. **Command & Control:** Channel to communicate and pass data between infected devices and their server.

6. **Actions on the Objective:** Different motives; data exfiltration, infrastructure destruction, create fear/extortion.
TARGET – YOU!

- Home
  - Internet of Things
  - Wi-Fi
  - Family
  - Smart Phone

- Travel
  - Vacation
  - Business/Conferences

- Work
  - Internet
  - Wi-Fi
  - Social engineering
  - BYOD

- Public
  - Wi-Fi
  - Theft
RANSOMWARE
FEDERAL & STATE LEGISLATION

• Federal
  • HR 1560, Protecting Cyber Networks Act - Rep. Devin Nunes (R-CA)
  • HR 1731, National Cybersecurity Protection Advancement Act - Rep. Mike McCaul (R-TX)
  • Cybersecurity National Action Plan – President Obama

• State
  • 47 states have established “data breach notification” laws to inform consumers
  • Maryland – Chapter 304/SB 676, all counties and municipalities to have reasonable security policies – Gov. Martin O’Malley (D-MD)
MUNICIPAL LEADER RESPONSIBILITIES

- Understand the Cyber Environment
- Think Strategically
- Understand Risk
- Adapt Best Practices
CYBERSECURITY MITIGATION STRATEGY CHECKLIST

- Risk – based approach
- Prioritized
- Define security baselines
- Information Sharing
- Incident Response capabilities
- Increase Awareness
- Public/Private Cooperation
Develop a clear structure for assessing and managing risk
Assess threats by using threat modeling
Document and review risk acceptance and exceptions
Make assessments and management of risk an ongoing process
Educate leaders to understand and support priorities
Consider resiliency
Leverage procurement processes to reflect priorities and risks
CYBERSECURITY MITIGATION STRATEGY CHECKLIST

Define security baselines

- Establish minimum security baselines
- Define clear roles and responsibilities for supporting a security baseline
- Establish a system for continuous security monitoring
CYBERSECURITY MITIGATION STRATEGY CHECKLIST

- Set expectations for sharing threat and vulnerability information
- Create a cross-city mechanism for sharing
- Run Cyber drills to test game plans
- Emphasize privacy and civil liberty protections in threat information-sharing
- Apply relevant national or international standards for information-sharing

MS-ISAC: Multi-State Information Sharing & Analysis Center
CYBERSECURITY MITIGATION STRATEGY CHECKLIST

- Create a Computer Emergency Response Team (CERT)
- Create clear ownership
- Engage private sector and national resources
- Enable consistent incident classification
- Test incident response capabilities and processes
CYBERSECURITY MITIGATION STRATEGY CHECKLIST

Increase Awareness

- Develop public awareness campaigns
- Cultivate employee development and workforce training programs
CYBERSECURITY MITIGATION STRATEGY CHECKLIST

- Take advantage of private sector resources
- Partner with universities
- Sponsor events to connect the public and the private sector
- Promote law enforcement cooperation while protecting privacy
- Create a culture of technology innovation

Public/Private Cooperation
Unusual Water Quality Scenario

- **Background:** It is summer in Emerald City. The end of the city’s fiscal year is approaching, and budgetary cutbacks within the city and the water department have resulted in several city employees being laid off.

- **The Event:** A water (or wastewater) utility worker, angry that he has lost his job, realizes that he is still able to remote into the Emerald City Water (or Wastewater) Treatment Plant’s SCADA system. He decides to infect the SCADA system with a computer virus to cause system malfunctions.
Spear Phishing Email Attacks Scenario

**Background:** Phishing’ emails are exploratory attacks in which criminals attempt to obtain victims’ sensitive data, such as personally identifiable information and/or network access credentials. These attacks open the door for further infiltration into the network. Phishing typically involves both social engineering and technical trickery to deceive victims into opening attached files, clicking on embedded links, and revealing sensitive information.

**The Event:** A town clerk received a seemingly legitimate email requesting they validate banking credentials. The overworked clerk clicked on the link and enters personal information.
SCENARIO CHARLIE

Ransomware Scenario

• **Background:** Ransomware operates by infecting a machine with malicious code, and executing that code to encrypt the contents of that machine and hold them hostage for a ransom of ~$300-$1,200. Once the ransom is paid, the attacker typically decrypts the data and returns the files on that machine to the user, though the longer someone waits to pay, the more money they have to spend to regain access to files.

• **Scenario 1:** Ransomware infects a machine, and then uses that machine as a gateway to hold an organization’s network hostage.

• **Scenario 2:** Ransomware infects a single machine, and then finds its way up to the cloud to encrypt and ransom whatever data it can find.
CYBERSECURITY INSURANCE

• Why have it?
• Providers
  ➢ LGIT, Travelers, Hiscox
• Coverage
  ➢ Privacy & Cyber Security Liability
  ➢ Media Communication Liability
  ➢ Data Breach Response/ Crisis Management Costs
  ➢ Cyber Extortion Damages
  ➢ Privacy Regulatory Defense, Awards and Fines
  ➢ Payment Card Industry Fines

Source: LGIT
QUESTIONS?