Cyber Security Check List

1. Employ the TRC Approach

Threat Assessment, Remediation, Continuous Monitoring

Identifying what types of cyber threats face your city is critical to creating a workable and realistic prevention plan. These threat assessments should include an acknowledgement of the range of cyberattacks that could compromise these areas; from accidental, to malicious software and online fraud, to full-blown terrorist activities. Once a threat assessment has been completed, a city should immediately remediate any issues the threat assessment raises. Finally, the quickest and easiest investment a city should make is retain continuous monitoring services, especially in the areas that were identified as vulnerable by the threat assessment.

2. Set Clear Security Priorities

Not everything can be deemed a security priority. While everything that a city does is important, there are certain services and information that are critical to a city's functioning. Evaluating which information and systems must be a priority will be a difficult, but will be easier once your city conducts a threat assessment. While the Association does not have a formal recommendation as to what systems and information a city should prioritize securing, the Center for Internet Security (CIS) has identified certain critical security controls that may be helpful when developing cyber priorities. The can be found here.

3. Create Incident Response Measures

Attacks that create vulnerabilities for high level priorities will call for a much different response than attacks that compromise low-level priorities. Understand these differences and create the appropriate response measures for different priority levels. Examples of response measures include:

- ❖ Creation of Computer Emergency Response Teams (CERT)
- ❖ Create External Incident Classifications
- ❖ Conduct Test Drills Regularly

4. Invest in Training Employees and Updating Internal Security Measures

Short of a terrorist style, cyber-attacks, most cyber incidents occur because of the failure of employees to operate in a secure manner while online and using city networks. Some examples of employee training and internal security measures that can easily be taken are listed below:

- ❖ Ensure anti-malware software on devices is up to date
- ❖ Limit access to internal Wi-Fi networks with credentials and encryption software
- ❖ Require two factor authentications (2FA) on all sensitive system used by employees
- ❖ Require strong passwords and regular password changes that prevent reuse of previous passwords.

5. Secure Sources of Funding for Updates to Cybersecurity Systems

Cybersecurity is not an inexpensive investment, but it is likely a cost effective one. Cities should consider creating a shared services model to help share the cost burden amongst multiple municipalities. It is the committee's recommendation that cities and agencies begin evaluating and implementing a shared-services model with other similarly sized and similarly-situated cities and agencies in Orange County. This shared services model will help control costs amongst cities, and will lead to a more holistic regional approach to cyber security in Orange County. Any city interested in a shared services of JPA approach to cyber security should contact the Association for assistance.

Please email Kelsey Brewer, Policy Manager for the Association, for a copy of ACC-OC's Cyber Security and Cyber Resiliency White Paper. She can be reached at kbrewer@accoc.org