TO: ACC-OC Board of Directors

FROM: Kelsey Brewer, Policy Analyst

DATE: July 26 , 2017

SUBJECT: Cybersecurity White Paper (Approved Draft)

---

## Executive Summary

On the following pages, the ACC-OC Infrastructure and Technology Committee has outlined key cyber-security and cyber-resiliency issues that focus specifically to local governments and agencies. While the recommendations outlined in this white paper are critical to achieving security for Orange County Cities and agencies, many of them will require a commitment of time and resources, and may take many months to implement effectively. To that end, the Infrastructure and Technology Committee wanted to highlight three steps at the beginning of this paper that every single city and public agency in Orange County should take immediately to secure their cyber infrastructure. They require a relatively minimal investment from cities and agencies, and will help inform and improve the outcomes from the recommendations made on later pages in this document. These key steps are:

1. **Threat assessment**
2. **Remediation**
3. **Continuous Monitoring**

The Infrastructure and Technology committee recommends that cities and agencies bring in a firm to conduct a comprehensive threat assessment of specific vulnerabilities within the cyber infrastructure. By completing this threat assessment, cities and agencies will be better able to understand what their vulnerabilities are when implementing further recommendations, such as what type of employee training to conduct internally. After completion of a threat assessment, it is critical that cities and agencies take these findings seriously and immediately begin implementing remediation strategies as soon as possible. Firms will often offer specific remediation recommendations after their evaluation, and some, if not all, can be completed internally by IT staff. Finally, when a city or agency does decide to invest in its cyber-security infrastructure, it is important that this investment include an

emphasis on continuous monitoring. Continuous monitoring is the best tool cities and agencies have to ensure that basic cyber-infrastructure is being protected immediately, while also deciding what additional updates and security strategies need to be implemented in the long term.

Finally, the ACC-OC Infrastructure and Technology Committee would like to emphasis its understanding of the high costs associated with cyber-security and resiliency. While a threat assessment is within the realm of financial possibility for most cities, longer-term investments, like the ones outlined on the following pages, will be much costlier. 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.

## Introduction

In the evening of April 7th, 2017, the residents of Dallas, Texas were startled to hear emergency sirens beginning to wail throughout the city. Soon that confusion turned to panic as all the city's 156 outdoor emergency sirens came online and continued to blare into the early morning hours on Saturday. The city was, in a word, unprepared. Emergency response teams were deployed across the city in an unorganized fashion, 9-1-1 call centers were inundated with panicked calls from residents wondering if the city was under attack or if they should evacuate, and most importantly no one seemed to know what had caused the system malfunction or how to make it stop.

It became clear the following morning that the city had suffered one of the most visible cyber-attacks on a local government entity in recent memory. While there was no lasting financial or physical damage caused by the attack, there was the revelation of how vulnerable the city's communication and information infrastructure was. And, perhaps most importantly, how unprepared the city was to respond to such an attack.

♦ ♦ ♦ ♦

As cities continue integrating smart technology into the day to day functions of local government, the need for strong safeguards against attacks are critical to maintaining system integrity. This white paper outlines strategies and tools for local governments to use when evaluating the effectives of their security measures. The paper will focus on strategies and tools for two major areas of security concern: Cybersecurity and Cyber Resilience.

While the two terms may appear similar, they refer to a different set of procedures, policies, and responses a city must consider when evaluating their cyber-attack readiness. As Paul Nicholas, Microsoft Senior Director of Global Security Strategy and Diplomacy explains,

> "Cybersecurity is about protecting the confidentiality, integrity, and availability of data, ICT[1] systems, and ICT infrastructure. Cyber resilience is about the

[1] Information and Communication Technology (ICT) is an extended term for information technology (IT) which stresses the role of unified communications and the integration of telecommunications (telephone lines and wireless signals), computers, as well as necessary enterprise software, middleware, storage, and audio-visual systems, which enable users to access, store, transmit, and manipulate information.

ability of ICT systems to continue delivering their intended output in some form, even if cybersecurity is failing or has fail."

Understanding and implementing standardized responses to these different set of challenges will be critical to the overall success of a city maintaining its ICT systems and infrastructure. To fully appreciate the importance of this task, it is important to first understand how the evolution of "smart cities" have changed the security landscape of municipal government.

♦♦♦♦

**Smart Cities**

Integration of technology into local government functions has been increasing at a exponential rate in the past few years. By using technology to automate and improve city services, municipalities and local agencies have saved time and money when administering these services, while also improving the quality of life for residents through efficiency and dependability. While smart city technology may seem innocuous, it touches the many critical functions carried about by local governments and agencies. Some example smart city technology are listed in the chart below.

*Table 1: Smart City Technology in Orange County*

| **Smart City Technology** | **Definition** | **Orange County Example** |
|---|---|---|
| Smart Traffic Control | Traffic lights and signals that adapt based on volume and real time traffic conditions | OCTA's Traffic Light Synchronization Project |
| Smart Parking | Residents can use apps to find available parking, pricing, and pay in real time | City of Newport Beach's collaboration with ParkMobile App |
| Smart Public Transportation | Real time data about schedules, arrivals, and delays. The ability to pay fares from mobile devices | Anaheim Resort Transportation App or<br><br>OC Bus Mobile Ticketing App (OCTA) |

| | | |
|---|---|---|
| Smart Energy Management | Smart grids can deliver energy based on needs, smart meters can "talk" to the smart grid to schedule energy supplies at a specific time for lower cost, and can be turned on and off remotely | Irvine Smart Grid Demonstration (ISGD)<br><br>SoCal Gas Smart Meters |
| Public Safety | Security and communications devices that provide real time information on what is happening and where | Orange County Interoperable Communications Systems<br><br>City of Dana Point Community Alert Siren System |
| Open Data Systems | Data is shared (sometimes in real time) by governments as part of transparency efforts. Often this data is available in smart phone app | City of Huntington Beach Open GIS Data project |

While there are a multitude of examples not included in the chart listed above, this does provide a general idea of the how much technology has become intertwined with basic day to day services offered by cities and regional entities. This chart also demonstrates how susceptible the most basic of services are to cyber-attacks. While a parking app being shut down via a cyber-attack would, at best, be a general annoyance, having someone compromise the integrated street light systems in Orange County could raise serious public safety concerns. As cities continue to modernize and use technology to streamline their functions, it is important to keep in mind that this modernization requires equal attention given to how to protect this technology from cyberattack.

**Local Efforts**

While Orange County remains in need of serious Cyber-Security advancement there are examples of cyber-security initiatives taking place throughout the county. Examples of cybersecurity at the Orange County department and agency level include:

- The Sheriff's cybercrimes unit, which handles cybersecurity oversight for the Sheriff's department.
- The DA's cybercrime investigation unit.
- The Health Care Agency (HCA) recently purchased a user "sandbox" system (secure and contained) to detect and arrest malware.
- The Sheriff's department mobile units are now password protected and data is encrypted in transit.
- The HCA and the Social Services Agency (SSA) are moving to full disk encryption on all laptops

As the Orange County Grand Jury report entitled *Orange County's Digital Data: Is It Protected From Cyber Attack?, n*otes, *"*some Orange County agencies and departments have employee exit procedures that reflect best cybersecurity practices, but none are comprehensive." While this is certainly a positive development at the County level, the implementation of some of these practices have failed to reach the city level where some sensitive data is most vulnerable. In order to have a comprehensive cyber-security strategy, the cities in Orange County must be a major component in the effort to implement best-practices county-wide.

♦ ♦ ♦ ♦

**Strategies and Policies for Cybersecurity**

The following recommendations are specific to strategies to prevent and ward off cybersecurity as defined on page two of this white paper. They are meant to focus on protecting the confidentiality, integrity, and availability of data, ICT systems, and ICT infrastructure, and are proactive and educational-based in nature.

*Recommendation #1: Evaluate Your City's Threat Landscape*

Identifying what types of cyber threats face your city is critical to creating a workable and realistic prevention plan. The uniqueness of each Orange County city means that while there will be universal risks for all 34 cities, the threat landscape between cities will likely differ to some extent. For example, the siren systems in place for Orange County's coastal communities will likely be a target identified by a threat landscape assessment, while more

inland cities may find that their local transportation networks are of special concerm. Still, all threat landscape assessments should focus on three major areas:

1. **Data**
    a. Police Records
    b. Health Records
    c. Permitting Records
    d. Financial Records
2. **Systems**
    a. Emergency Communication Systems
    b. Education Systems
    c. Law Enforcement Systems
3. **Infrastructure**
    a. Electrical Grids
    b. Fiber networks
    c. Water Transportation Networks

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. Understanding your specific city's vulnerabilities will allow you to set clear priorities for cyber management later on.

| Threat | Examples | |
|---|---|---|
| Passive | Unintentional actions | Exposure to malware through email or websites |
| | | Receipt of spam email or phishing |
| | Under-resourcing | Unprotected systems |
| | | Unclear mitigation strategies |
| | | Undefined response capabilities |
| | | Lack of clear ownership |
| Active | Cybercrime | Fraud |
| | | Distributed Denial of Service |
| | | Theft of intellectual property or finances |
| | | Abuse or damage of ICT systems |
| | | Damage to critical infrastructure |
| | Natural hazards | Typhoons and hurricanes |
| | | Earthquakes and tsunamis |
| | | Floods |
| | | Tsunamis |
| | | Accidental cutting of undersea Internet cables |

Microsoft provides a very general outline of what a potential threat assessment may look like, though any model that clearly identifies specific risk and vulnerabilities associated with your specific city is acceptable for this recommendation.

*Recommendation #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 necessary task when it comes to deciding which employees to train first and where to invest precious resources to strengthen security systems. 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.

*Recommendation #3: Create Incident Response Measures*

By creating a set of cybersecurity priorities, you will be better able to develop a set of short term and long-term response measures. Attacks that create vulnerabilities for high level priorities will call for a much different response than attacks that compromise low-level priorities. For example, a widespread attack to a city's power grid would most likely need to trigger a response from a city's public safety department and coordination with outside agencies (both private and public), while an isolated attack to the computers within a city's recreational department would mostly likely only require an internal response from the city. Creating specific guidelines will prevent confusion as to how employees should respond or how resources should be allocated in times of crisis. Incident Response Measures can include:

1. Creation of Computer Emergency Response Teams (CERT)
    a. These teams should include experts from the private, government, and academic worlds, and are meant to help coordinate responses in case of an incident.
2. Create External Incident Classifications
    a. These classifications will determine when it is appropriate to notify the city of an incident or when it is important for the city to provide resources to external entities as part of the general response to an attack. While this white paper is meant to highlight the vulnerabilities that exist within functions controlled by a local government, it is possible that an attack could target non-government controlled resources that will still impact a municipalities' ability to function. For

example, no Orange County city operates a water district but a threat to the local water transportation networks would certainly impact the ability of a city to operate. Classifying such an attack as “response-worthy” for a municipality will help streamline resources if necessary.

3. Test Drills
    a. Just like disaster preparedness, running test drills of response systems is critical to evaluating the effectiveness of current cyber-attack responses. Test drills should occur on a periodic basis and should evaluate employees’ response and ability to quickly coordinate internally and externally.

*Recommendation #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. For example, a common tactic used by hackers is social engineering, where a hacker uses psychological manipulation to get an employee to divulge information they otherwise would not be inclined to share, such as social security numbers of fellow employees. By posing as an authority figure, such as a supervisor, a hacker may receive access to information that was otherwise protected by security systems in place. Most of these incidents are preventable with the right training, such as instructing employees that they are never allowed to send sensitive personnel information via email, regardless of who is requesting the information. By training employees and holding them accountable to strict security measures, a city can dramatically decrease the likelihood of becoming vulnerable to a cybersecurity incident. 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
- Backup files and data to the cloud as often as possible
- Employee training and education about social engineering attacks and how to recognize them
- City-wide internet and computer usage policies

- Conduct regular security checks and campaigns to identify offenders
- Mandatory training for repeat offenders, as well as disciplinary action
- Require system administrators to have separate user profiles for admin activities
- Regularly check what ports are open on internal networks and their behaviors
- Separate the city network for guest and internal users
- Pay attention to mobile app permissions and access, some will access to very private, personal and proprietary information a city would want to remain confidential.
- Inventory the devices and their IP addresses on the city network. Remove ones that do not belong there.

This list of possible steps is not meant to be exhaustive. Once a city completes their threat assessment landscape, it is likely that additional internal security measures and training will become necessary.

Additionally, cities can choose to develop an internal, ransomware policy that would allow for a quick response to security breaches. In some cases, it may be more cost effective to pay a ransom then to allow for sensitive information to be compromised publicly. However, there is no uniform agreement amongst cyber security experts if a ransomware policy is necessary or an effective means of promoting cyber-resiliency. ACC-OC is not formally recommending that cities develop such a policy, but rather to review, in consultation with their city attorney, what services may rise to the level of critical designation and therefore may require a flexible and responsive ransomware policy.

When developing an internal ransomware policy cities should consider the following tiers of response that would allow for a timely turn around during a security breach:

- The amount an IT Manager can sign off on without City Manager or City Council approval
- The amount an IT Manager can sign off on with City Manager approval
- The amount a City Manager can sign off on without City Council approval
- The amount a City Manager can sign off on with Mayor approval
- The amount that will require the approval of the entire City Council in emergency closed session.

Again, balancing the long-term cost of a comprehensive security breach is key. Developing a ransomware response policy may save a city thousands of dollars and a public relations debacle.

*Recommendation #5: Secure Sources of Funding for Updates to Cybersecurity Systems and Retention of Cybersecurity Talent.*

Cybersecurity is not an inexpensive investment, but it is likely a cost effective one. As explained by Cristin Goodwin, Senior Attorney for Microsoft,

> "For most cities, balancing cybersecurity with other budget priorities will be a challenge, albeit one that can be lessened by understanding the return on investment from cybersecurity measures. In 2014, the Center for Strategic and International Studies produced *Net Losses: Estimating the Cost of Cybercrime; Economic Impact of Cybercrime,* which estimated that the likely cost to the global economy from cybercrime was $400 billion annually—or 8 percent of the estimated global GDP. To assess the return on investment for cybersecurity measures, a city should consider the economic impact of cyberattack on citizens, law enforcement, local businesses, and city administration."

Sponsoring legislation meant to support cybersecurity funding for local agencies, educating elected officials on the importance of cybersecurity investments locally, or even just prioritizing the security features of new purchases when retiring old systems are all ways that cities can begin finding the revenue sources necessary to make cyber security a priority.
Additionally, 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.

♦♦♦♦

**Strategies and Policies for Cyber Resiliency**

As mentioned earlier, there is a distinct difference between cybersecurity and cyber resiliency. Though intimately connected, these differences require a different set of strategies and policies for achieving security within cities. The following recommendations are specific to strategies meant to promote cyber resiliency as defined on page two of this white paper. They are meant to protect and preserve the ability of ICT systems to continue delivering their intended output in some form, even if preventative cybersecurity measures are failing or have failed.

*Recommendation #1: Prioritize Critical Services*

This recommendation is related to *Cybersecurity Recommendation #2* listed on page five, though it differs from the preventive nature that recommendation is meant to focus on. The prioritization of critical services is about what response a city will have once *preventive measures* have failed or are failing. In reality, this recommendation is more likely to be closely related to *Cybersecurity Recommendation #1* listed on page four. Understanding the specific threat landscape of your city may help you anticipate what internal and external threats an attacker is most likely to target, and will help a city plan which of those targets rise to the level of a critical service during a cyber incident. In the event of a multifaceted attack, it is critical to ensure resources are being used in a methodical nature instead of being spread so thin to the point that they are no longer effective.

For example, a hypothetical attack may unfold like this:

> *A hacker has gained access to the traffic lights operating within a particular city, while also simultaneously taking the city's website offline. It may seem that both attacks affect the critical services a city provides; one affects the transportation infrastructure of the city and the other affects the external communication system of the city. However, by prioritizing critical services, the response team would know to look for which attack provides the most flexibility in terms of a response. While the communication system of a city is a critical service, the ability for the city to use alternative forms of communication with residents, such as social media, would allow them to prioritize scarce resources to the transportation infrastructure attack.*

During an attack, all services offered by a city may seem critical, but by identifying criteria for what is to be considered a critical service during an attack and providing guidelines for prioritizing services when multiple city functions are compromised, cities will be able to more methodical distal what actions should be taken first.

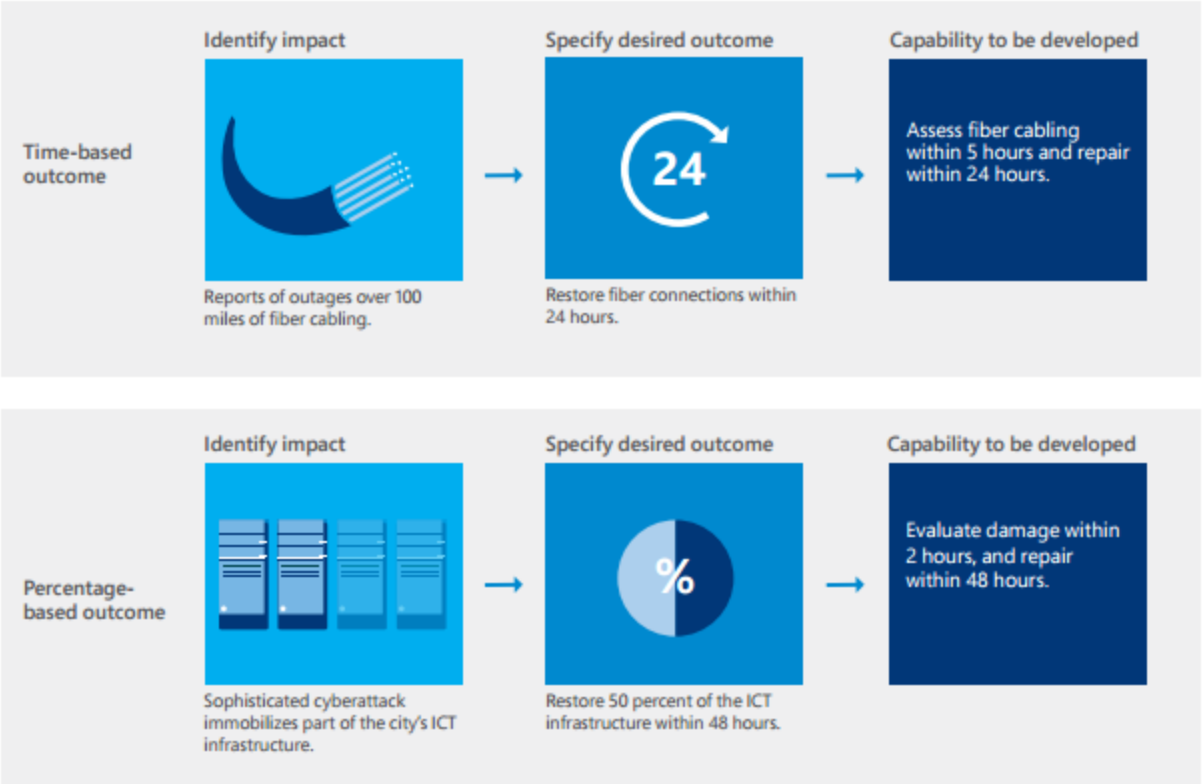
Listed below are questions recommended by Microsoft's Cyber Security Research Team that may be help you classify, prioritize, and plan to recover critical services

- *What critical services does the city need to protect most and recover first?*
- *Who is responsible for each of these critical functions?*
- *How long can certain services be offline or interrupted before they become critical—1 hour, 5, 24, 72?*

*Recommendation #2: Establish Desired Outcomes and then Test the City's Capability to Reach Those Outcomes*

This recommendation borrows heavily from FEMA's definition of desired outcome which is as follows, "Desired outcomes describe the timeframe or level of effort needed to successfully deliver core capabilities. Capabilities are only useful if communities can deliver them in a timely and effective manner."

A resiliency response plan is only as effective as a city's ability to deliver said response. By creating time and percentage based outcomes, cities will be able to evaluate their capability to achieve said outcome. An example is listed below:




When creating desired outcomes for external threats such as transportation infrastructure, energy infrastructure, and communication infrastructure, it is important that cities develop these desired outcomes in collaboration with all relevant government agencies and private companies that may play a significant role when achieving the desired response outcome during an attack.

While it may seem that this recommendation is specifically meant to address attacks that are meant to destabilize a city, this model is also useful when dealing with non-terrorist related cyber-attacks. For example, having a specific desired outcome for a situation when ransomware has infected a city's internal network will allow for a city to respond to internal threats just as effectively as external ones.

*Recommendation #3: Clearly Define Roles and Responsibilities*

Once an attack has occurred and preventative cybersecurity measures have failed, it is important to develop a protocol for who will lead the resiliency response. These roles and responsibilities may challenge traditional chains of command. Individuals may be placed in positions of authority based on expertise and knowledge that are not used to serving in these roles. However, this clear classification of responsibilities is necessary to ensure that competition amongst departments or multiple municipal agencies is not occurring. The lack of this response structure could either lead to critical information not reaching the correct people, or a delay in response time due to a lack of direction and communication.

Even in non-critical cyber-attacks, it is important for there to be a strong defined chain of command to ensure that even the most minimal of system compromises are dealt with efficiently, with as little impact to the city as possible.

♦ ♦ ♦ ♦

**Conclusion**

In a way, a more technologically integrated society is a more vulnerable society in the age of cybercrime and cyberterrorism. However, there are straightforward steps that cities can begin taking to protect their internal networks and systems, and proactive steps they can consider when collaborating with other government agencies and organizations to prepare for external, multifaceted cyber-attacks.

As the world continues to become more interconnected, we all share the responsibility of securing cyberspace for our residents, businesses, and employees to the best of our collective ability.