



A DIVISION OF FUSION LEARNING PARTNERS

Introducing PTI's Newest Tech Assessment & Advisory Service

Cyber Awareness Simulation for Public Managers

A cyberattack or breach of a local government's IT systems can have a devastating impact on its ability to function at all levels of operations and service delivery. Such an event would likely cripple business operations as well as lead to a loss of public confidence and support. Based on recent experiences with other local governments, a cyberattack is now considered a public emergency, requiring a thoughtful, legal, and coordinated governmentwide response.

According to Public Technology Institute (PTI), cybersecurity continues to rank as the No. 1 priority for technology executives. Unfortunately, cybersecurity as a priority may not resonate within other executives and leadership within a local government. All too often cybersecurity is viewed as an IT "responsibility" versus an issue or priority that impacts every department and function of government operations and service delivery.

To help local government officials outside of the IT organization develop a better understanding of what it is like to experience a cyberattack, PTI is offering a virtual cyber tabletop exercise where the PTI team of experts – staff and volunteer cyber executives from other local governments – will take participants through a simulated cyberattack and make recommendations as to how to improve the jurisdiction's incident response.

Background

Imagine finding out that your jurisdiction's IT systems have been hacked for ransomware and you have just 72 hours to pay the ransom. What are the questions that need to be answered and the decisions that your organization's leadership need to consider immediately?

- What do you tell the public?
- How do you communicate with staff if your IP phones are down?
- How and what do you communicate with elected leaders and staff?
- Who do you contact from state or federal agencies?
- If you have cyber insurance, what is covered and what obligations are you required to take based on your policy?
- What data backup and recovery systems do you have in place?
- How do employees and vendors get paid during the system down time and recovery?
- Do you pay the ransom or not, and what are the implications of each?

The PTI Cyber Incident Team

The PTI Cyber Incident Team is comprised of staff and volunteers who are both knowledgeable in cyber governance and cyber best practices as promulgated by the U.S. Department of Homeland Security as well as MS-ISAC. Team members have included CCISP (Certified Cyber Security Professional) certifications.

The Cyber Assessment Program and Simulation

The program can be fully executed in as little as 30 days and involves the following steps:

1. The PTI Cyber Incident Team meets with the exercise leader or person(s) initiating this exercise. This is usually done through the IT department and includes the IT executive and top IT staff.
2. The PTI Cyber Incident Team reviews all applicable policies, regulations, and written SOPs, including Disaster Recover Plans, COOP, and any Breach Response policies provided by the jurisdiction. This step is critical in preparation for the exercise.
3. The PTI Cyber Incident Team conducts a live virtual simulation lasting no more than 90 minutes. The objectives are:
 - a. To raise cybersecurity as a priority with jurisdiction officials and to expose these officials to realistic and time-sensitive experiences and decision making.
 - b. To provide a realistic experience for those involved to improve planning and response for a real incident.
 - c. To build a strong and unified understanding among key players so that, if and when a real attack occurs, everyone has an understanding of their respective roles and responsibilities.
4. Immediately following the virtual exercise, the PTI Cyber Incident Team meets with top IT staff to provide feedback and recommendations as to their actions during the exercise.
5. Within two weeks of the exercise, the PTI Cyber Incident Team prepares the After-Action Review/ Report Card that contains helpful critiques, recommendations, and suggestions, and provides a list of relevant resources to better protect and respond to cyber incidences. This includes a list of actions steps that should be taken with helpful explanations.

Program Cost

The cost of this program is \$12,000 for PTI members and \$15,000 for non-members for a virtual exercise; in-person training is billed as plus travel and lodging plus additional time required for travel.

For more information about the PTI Cyber Assessment Program, contact:

Dale Bowen
202.626.2456
dbowen@fusionlp.org

**PTI is a nonprofit association dedicated to serving the needs for technology leadership and professional development for cities and counties throughout the nation.*

