CompTIA Public Technology Institute

BEST PRACTICE BRIEF

Developing Your Local Government Cyber Road Map:

HOW FEDERAL FUNDING CAN HELP

With the Infrastructure Investment and Jobs Act recently signed into law, local governments will, for the first time, receive federal funding to enhance cybersecurity programming. Over $1 billion will be distributed to state and local governments over the next four years, with cities and counties expected to get 80% of this funding. This funding will support efforts by state, local, tribal, and territorial government to improve cybersecurity needs by securing their networks, assessing their cybersecurity vulnerabilities, and building up their cybersecurity workforce.

Now is an opportune time for local government IT and cyber executives to reexamine their cybersecurity standing and undertake a comprehensive review of their cybersecurity needs for new or updated initiatives and solutions.

Elected leaders and management will quickly ask the question "where do we start?" Of course, every jurisdiction is different, with unique needs, priorities, resources, staffing and expertise.

There may be a rush to spend, and this will likely come from outside the IT department. Recognizing this pressure, it is important to show leadership and the community that there is a strategy in place—a road map—for how the public's money will be spent.

Following are recommendations that CompTIA Public Technology Institute member IT executives suggest officials consider as your local government expands and improves upon your current cyber posture. These can be tailored to fit the specific needs of your organization and factored into the development of your cyber road map.

It is important for elected leaders to be made aware that some initiatives will be on-going; your organization will have to pay annual fees, license renewals, and system updates over time—not for just one budget cycle.

IT executives might consider starting with a quick success; a one-time expenditure, for example, a cybersecurity tabletop exercise that takes leadership through what it will be like to go through a ransomware attack. This experience will be a "win" because it will get all departments involved and make cybersecurity an organizational issue - not just an IT issue.

Engaging elected officials in the development of your organization's cybersecurity roadmap will help to build momentum and ensure that cybersecurity is a priority.

The Starting Line

- It begins with your cyber team. Review staff competences and asses your team's capabilities. What professional expertise is lacking? What technical skills are needed? Because the cyber landscape is constantly changing, identify opportunities for staff training, to include certification and recertification educational programs.
- Your cyber team is on the front line of your cyber defense, dealing with a variety of challenges and on call 24 hours a day: It is important to monitor and boost your team's wellness.
- Consider what some might consider non-traditional approaches to bolstering your cyber team: apprenticeship and internship programs with local community colleges and universities.

- The pandemic and the move to remote work and service delivery shone the spotlight on the importance of broadband. If you haven't already reviewed as part of your remote work activities, assess broadband connectivity: Both internal (office to office or location to location) and external (resident input points of contact).
- Review GIS capabilities with an enterprise view; look for gaps in layers and coverage.
- Review equipment and device replacement policies.
- Reexamine your organization's mobile device management policies (this may have already assessed in the past two years as part of your remote work and access strategy).
- Conduct penetration testing and evaluate the security of your IT infrastructure by safely trying to exploit vulnerabilities.
- Review and update employee awareness and training processes. Training should be ongoing—not a once-a-year event—and all levels of officials, to include elected leaders, must be part of this training.
- Consider how the IT organization communicates with leadership about current cybersecurity issues and response; develop a template or model to follow in case of a security breach. The involvement of your elected leaders must be a part of every local government's overall cybersecurity strategy.
- Examine, on a routine basis, the security protocols and policies of your vendor partners.
- Review the latest frameworks and policy recommendations issued by federal government agencies. This direction can serve as building blocks for your planning efforts.
- If your organization has a cybersecurity insurance policy, ensure that you and your team, and leadership, are aware of what is required to respond in the event of an incident.
- Reach out to colleagues in neighboring jurisdictions to learn any trends or issues that they are experiencing, and to identify opportunities for collaboration.
- CompTIA Public Technology Institute is a strong proponent of state and local collaboration at all levels, particularly regarding cybersecurity. Reach out to your state IT leadership about information and resource sharing initiatives that are available.

The Finish Line

Over the past several years, surveys conducted by the CompTIA Public Technology Institute have shown that cybersecurity continues to rank as the number one priority for local government IT executives. The new funding provided by the federal government provides a much-needed financial assist to help local governments expand upon and improve cyber defenses.

We began this CompTIA Public Technology Institute Best Practice Brief with a look at the starting line. The race is on! The finish line is a living, thought-through, organization-wide cyber road map that involves elected leaders as cybersecurity champions.

Additional Resources

U.S. Department of Homeland Security, Cybersecurity and Infrastructure Security Agency

www.cisa.gov

CompTIA-PTI 2021 National Survey of Local Government Cybersecurity and Cloud Initiatives

https://comptiacdn.azureedge.net/webcontent/docs/default-source/research-reports/pti-2021-cybersecurity-report-final.pdf?sfvrsn=fbe93818_2

About the CompTIA Public Technology Institute

PTI merged into CompTIA in January 2019 yet remains a distinct and semi-autonomous membership and service delivery organization. Established in 1971 by the several major national associations representing state and local governments, PTI has been viewed as the focal point for thought leaders who have a passion for the furtherance and wise deployment of technology. PTI's initial funding was through a grant from the National Science Foundation. Today, PTI actively supports local government officials through research, education, professional development, executive-level consulting services, and national recognition programs. Visit www.pti.org.