Why should municipalities make network and data security a priority?

Next Century Cities

Internet Society

As of August 2019, ransomware attacks had already targeted more than 50 municipal governments this year. And as communities add more connected devices to their tech ecosystems and collect more data, the threat is ongoing. Experts now predict that the odds of a municipality becoming a target of a ransomware attack are one in four. Not only do attacks take local services offline and disrupt critical functions, but recovery can be extremely costly. Further, breaches of municipal data stand to expose sensitive information about residents. As municipalities manage existing networks and adopt new technologies, network and data security practices should be a top priority.

What can municipalities do to minimize risk?

Communities can minimize risk by being intentional about how and by whom networks and devices are used. Here are eight best practices for municipal governments to optimize security.

1. Set strong internal data policies

Only collect data that serves a purpose, and whenever possible, ensure that data is not personally identifiable. Be thoughtful when determining:

A. What data is being collected?
B. Where and how is data stored?
C. Who has access to sensitive information?
D. What safeguards are in place to intercept a breach?
E. Is data being sold?

2. Set strong internal security policies

Security requires all team members to be cautious about how they use technology in the workplace. Comprehensive security policies should address network connections, use of Internet of Things (IoT) devices, password parameters, use of encryption, and consistent data backups and software updates. Learn more about best practices for how individuals can keep the workplace secure in this factsheet.

3. Conduct staff trainings

Hold regular trainings for all staff members that address basic privacy, security, and network vulnerabilities as well as the specific actions that individuals can take to minimize risks, including internal policies such as those outlined above.

4. Backup data often

Having a recent, comprehensive backup of municipal data on hand can minimize the impact of a ransomware attack. Ideally, files will be backed up with both a Cloud provider and an external storage device, and backups should be disconnected from system computers and networks.

5. Run regular security updates

Ensuring that security patches and updates to network infrastructure are applied regularly can help prevent known threats.

6. Hold vendor partners to high privacy and security standards

It's critical to set privacy and strong security parameters for whenever new devices, software, or programs are being introduced into your network. Securing Smart Cities offers a guide to security considerations for selecting, implementing, and disposing of smart city technologies.

7. Apply MANRS actions to networks

If your city owns or operates its own network, it should become a member of Mutually Agreed Norms for Routing Security (MANRS), which sets concrete actions for network operators to take in order to eliminate common routing threats. If a new network operator wants to offer service in your community, you should encourage them to become a MANRS member as well.

8. Consider an insurance policy

While insurance can't prevent attacks, a policy can help mitigate risk and assist with the cost of recovering from an attack, natural disaster, or prolonged service outage (e.g. power outages). Many larger cities purchase their own cyber insurance policies, while smaller communities have the option of opting-in to pooled plans offered by associations.

Additional Resources

The Internet Society provides fact sheets on best practices for IoT and network security for individuals and enterprises, including Best Practices: Security & Privacy for Enterprises.

The Multi-State Information Sharing & Analysis Center provides cyber threat prevention, protection, response, and recovery resources for state, local, tribal, and territorial governments.

The National Institute of Standards and Technology published the Cybersecurity Framework which includes guidelines and recommended practices for municipalities of any size to develop their comprehensive cybersecurity strategy. The agency also publishes white papers and hosts events to provide additional training.