3 Steps to Effective Local Government Cyber-Security

Four years ago, the city of Atlanta launched a smart city initiative, hoping to improve municipal operations with integrated technology. The future looked bright. And then, in 2018, a ransomware attack crippled city infrastructure. One year and $17 million dollars later, Atlanta serves as a reluctant poster child for the necessity for robust local government cyber-security.

Anatomy of a Cyber-Attack

In 2019 alone, local governments and hospitals in the United States have reported 140 cyber-attacks. In fact, cyber-attacks have more than doubled since last year. These assaults have destroyed public records, disrupted healthcare and law enforcement and frozen online services.

In a typical ransomware attack, hackers access the municipal network either through a phishing email or by exploiting weak passwords. Once in, they encrypt files throughout the network, demanding a ransom in return for the decryption key. The city can either pay the ransom or restore from a recent backup and completely rebuild the system.

Hackers usually keep ransom demands fairly reasonable in order to encourage payment. However, the FBI recommends that victims refuse to pay. Not only does payment encourage more attacks, but hackers do not always deliver reliable decryption. In addition, they may leave additional malware hidden in the network to do further damage.

1. Understand the Obstacles and Risks

A number of risk factors common to municipalities complicate the security landscape. In the first place, local governments report a lack of sufficiently trained cyber-security personnel. Governments tend to pay less than the private sector and may experience difficulty attracting and retaining staff with the needed experience.

Secondly, as with many large organizations, municipalities frequently struggle to keep systems up-to-date. In the case of Atlanta, several reports indicated that the city had not applied fixes to known vulnerabilities. In fact, of the $17 million the city spent on recovery, roughly $11 million went to updating computers, tablets and smartphones.

Finally, many municipalities outsource services such as payroll and credit card processing to third parties. However, without adequate risk management procedures in place, the third parties introduce additional vulnerabilities.

2. Educate the Public and Decision Makers

Effective cyber-security requires investment in personnel, equipment and cyber insurance. And with limited budgets, local officials often prove reluctant to allocate sufficient resources to security efforts. Furthermore, cyber-security investment is not a “once and done” effort. Cities must stay up-to-date in order to remain secure.

Consequently, a critical step in improving local government cyber-security involves embarking on an education campaign. Voters, politicians and other decision makers must understand the cyber risks involved and the benefits of mounting a proactive defense.

Understanding the numbers can help. For instance, spending $50,000 in planned equipment and software upgrades now can avoid $100,000 in more costly emergency spending when an incident occurs.

3. Build a Security Strategy

Like Atlanta, cities across the country look to technology to solve pressing municipal issues. The internet of things (IoT) offers compelling solutions to untangling traffic snarls and delivering utilities more effectively, for instance. But without a solid security strategy, such efforts come with great risk. Necessary components of an effective security strategy include:

- **Backups** – Without adequate backups, cities have no recourse in the event of a cyber-attack. Establish a backup plan for both data and applications, storing the backups off-site and testing them for viability. When establishing a backup plan, keep in mind that any data newer than the most recent backup could disappear in an attack.

- **Risk assessments** – When considering implementing new technology, first conduct a risk assessment to identify any vulnerabilities. Then commit to addressing those risks as part of the implementation. In addition, conduct regular risk assessments of the entire system, including third parties.

- **Password management** – As in the case of Atlanta, weak passwords can provide hackers a door into the system. Implement a strong password management program. This should cover not only personal computers, but also mobile technology, system administration and smart devices on the network.

- **Recovery plan** – Develop a collaborative recovery plan for when, not if, an attack occurs. This plan expands beyond IT and should include procedures for every department. Specify first steps, communication protocols, and recovery priorities.

Local Government Cyber-Security Expertise

Navigating local government cyber-security can prove tricky in the unique municipal environment. When elected officials come and go, a trusted security partner can provide needed continuity.

With deep experience in government IT, eMazzanti can help local governments protect vital municipal services and sensitive data. From risk assessments to system monitoring and comprehensive security strategies, we provide the tools you need.