Cyber-security for Municipalities: Balancing Risk and Budget

From WannaCry ransomware to Russian collusion, cyber-warfare has taken a turn. According to Carl Mazzanti, President of eMazzanti Technologies, local governments are the new battleground. With increasing threats and tight budgets, cyber-security for municipalities requires a precarious balancing act from our public officials.

"Municipalities offer an easy target for bad actors," says Mazzanti. "They are relatively simple to breach, and they collect an abundance of valuable data, from taxpayer and credit card information to pension data."

Sacramento Recently Attacked

We may blithely assume that the personal and financial data we hand over to local governments sits securely behind impenetrable walls. But, this is not the case.

Just last month, a hacker breached the Sacramento Public Transportation System, demanding a one Bitcoin ransom (about $7,000) while shutting down the agency's website. When he failed to achieve his objective, the hacker deleted 30% of the data from the organization's server.

This was not an isolated incident, and more attacks will surely follow if proactive security measures are not taken. Unfortunately, some serious challenges make effective cyber-security for municipalities—the walls we want and expect—increasingly difficult to build.

Competing for Tax Dollars

City officials face the task of allocating limited tax dollars among multiple initiatives, from public safety to health and human services. Often, information technology (IT) accounts for less than 0.1% of the overall municipal budget.

As a result, municipalities typically struggle to offer the competitive salaries that skilled IT professionals demand. Those tasked to protect digital assets often lack sufficient training to counter increasing cyber threats.

Cities also find themselves restricted in their ability to modernize outdated systems. They want cutting-edge data security and know well the need to protect sensitive data. At the same time, they must address those needs within strict budgetary constraints.

Robust Security Policies Needed

In the municipal setting, multiple departments often share a common network with loosely- defined security policies. With separate reporting structures, accountability may fall by the wayside.

In addition, complicated regulations from various agencies result in varying compliance requirements. All too often, any formal cyber-security policies satisfy only the lowest level of security required.

To adequately protect data, cities and towns need clearly-defined policies for password management, email safety, managing risk from third-party vendors, and so forth. With the human element continuing to represent the greatest security threat, employees require both training and oversight.

Disaster Recovery Options

A cyber-attack or natural disaster can take down a municipal network or website in a matter of minutes, crippling public services and putting critical data at risk. While most cities and towns have incorporated some sort of backup system, many have yet to implement adequate business continuity plans.

From cloud-based storage to system replication with automated failover, municipalities that seek to strengthen their disaster recovery capabilities will discover numerous backup and security options. Expert guidance from outside the organization may be required to identify what is needed most.

Competing performance criteria must be evaluated and balanced. Centralized solutions offer simplified management. While, layered network security combines attack prevention with the ability to quickly detect and respond to breaches when they do occur.

Leadership and Public Support Required

To be successful, a cyber-security initiative must proceed from the top down, with a directive from the mayor, chief financial officer or other city officials. While both evolving threats and never-ending budgetary pressures present a challenge, municipalities can and must protect the data entrusted to them. The risks are too great.

Even with leadership from city officials, a successful cyber-security initiative requires funding. And, budgets require public support. When citizens voice their concerns over the safety of their data, IT will begin to receive a more adequate share of the funds available.

Increased Security and Responsiveness

By leveraging technology responsibly, a municipality can increase both security and responsiveness. Updated systems with enhanced cyber-security often result in reduced downtime and streamlined operations. That efficiency in turn builds trust with the citizens served by the municipality.

Making the best cyber-security provisions within budgetary restrictions requires careful planning. Towns looking to better secure digital assets or implement cloud solutions for municipal applications can work with knowledgeable government IT consultants. Certified security engineers provide expert guidance to achieve cost-effective cyber-security solutions.