infoedge

Ransomware Attack: Are your city's defenses ready?

A solid cyber-resilience strategy is the solution

Overview

Several recent examples show that any city in the US could be the next target for extortionists. The ramifications are acute and painful. Day-to-day operations can grind to a halt, preventing city services, contracts, and billing to continue without costly work arounds while you recover.

The problem is getting worse. A report from May 2019, by the cybersecurity firm Recorded Future, showed that publicly acknowledged ransomware attacks jumped 39 percent in 2018, with the first few months of 2019 continuing that trend. See *here* to read the report. Bringing data and operations into the 21st century drives municipalities and their citizens to rely more on their infrastructure being online. Cities undergoing transformational projects, including migrating to the cloud or using smart, internet-of-thing (IoT) devices and sensors are seeing increased efficiency coupled with a high risk of a disruptive incident.

Challenge

Ransomware is a favorite tool used by cybercriminals to lock you out of your systems and data until you pay up, at which point they (theoretically) restore your access. These cyber attacks are not new, but dealing with them **after** the fact is becoming costly, especially when preventative actions can go a long way toward keeping you out of the crosshairs.

Our Approach

Be resilient. Be proactive!

We get it, municipal budgets are tight. However, the incident frequency is tipping the risk / reward tradeoff of ignoring these issues badly out of favor.

The most resilient environments are those where proactive defenses are implemented, balancing risk, resources, and reality. Similar to the planning you do to prepare for natural disasters the objective is to start risk mitigation where you get the biggest bang for your buck and enable faster recovery when something inevitably does happen.

How can we take this mindset & help protect against impact of Ransomware?

- Know where your data and most sensitive systems are. Go further here with a **Data Governance** model to help you make the most of that data.
- Create a **disaster recovery** and **business continuity plan** which includes regular **backups** of your critical data. Practice this plan regularly. When ransomware hits, you can rebuild the system and go right back to work, without paying them a dime.
- Manage vulnerabilities through a robust **patch management** process. Missed security patches is one of the top ways that ransomware gets onto a network.
- What is your **municipal policy** that covers a ransomware event? Do you pay the ransom or wait, with each day costing citizens more and more? Are your citizens prepared to pay that cost?
- **Educate** your staff to steer clear of clickbait, phishing and other scams which are enticing entry points for ransomware.

In Conclusion

Cyber criminals are always seeking to be a step ahead and becoming a target, for cities across the world, is not a matter of if, but when.

Over-reliance on technology or insurance alone to solve cyber issues is doomed to fail. It takes a balanced approach utilizing **People, Process, and Technology** to achieve security while improving operational resilience. The steps outlined above can make a major difference in your preparedness for ransomware attacks.

The challenges will continue to grow. Solutions tailored within the context of your data, environment, and risk landscape can make the difference of “thriving” vs just “surviving” given an adverse event.

Contact us to learn more about how Governance, Risk, and Compliance services can help improve your resilience. Let us conduct a half-day risk workshop with your team to define and prioritize actionable projects to maximize defenses and minimize impact. Succeed in the information economy today and in the future.