CompTIA | pti Public Technology Institute

BEST PRACTICE BRIEF

# Cybersecurity and Elected Leaders:

## HOW A RANSOMWARE ATTACK IMPACTS YOU

Local governments are prime targets for a ransomware attack. Every day your government's IT systems are probed by individuals and organizations looking for a weakness, an opportunity to gain entry to your computer systems and hold your government hostage. Cyber criminals want to prevent your access to the large amount of data that your government holds: social security numbers, tax information, financial records, and other confidential information of residents and businesses.

**Cybersecurity is about data protection**

Your government manages a large amount of data to include resident social security numbers, tax information, financial records, etc. Cyber criminals want access to this data – to steal it or to hold access to it hostage.

City and County IT officials with the non-profit CompTIA – Public Technology Institute, a national, non-profit organization that focuses on technology issues impacting local government, created the following advisory specifically for elected leaders. The intent: To engage with elected leaders on the importance of having a sound cybersecurity strategy within your organization and to help provide some guidance when – not if – a ransomware attack occurs.

**What is ransomware?**

Ransomware is a form of malware designed to encrypt files on a device, rendering any files and the systems that rely on them unusable. Malicious actors then demand ransom in exchange for decryption.

**What is the impact of an attack?**

- A ransomware attack means not being able to access your government's IT systems and infrastructure, service to your residents and business community will be limited and could lead to the loss of data.
- Your government could pay thousands of dollars in ransomware and spend millions of dollars and months of staff resources to restore systems.
- While IT systems are down, you are most likely unable to process fees thereby losing thousands of dollars in revenue from not being able to process fees and payments.
- Your government's bond rating could be negatively impacted.
- Future insurance premiums could rise, or the inability to secure insurance in the future.
- Perhaps, most important: Resident and business confidence in your government and your leadership could be negatively impacted.

**As an elected leader what can you do to ensure a strong cyber posture?**

- Managing cyber is about managing risk. Your government's cybersecurity efforts should be considered part of your risk management efforts.
- Be involved: Be familiar with your government's cyber strategy. This includes having a plan for continuity of operations in the event your technology systems have been compromised or are unavailable for some period of time.
- Be aware: Participate in cyber education and training programs just as staff does.
- Stay informed: Talk to your cyber team and IT leadership about the key security issues your government is facing.
- Invest in cybersecurity: Whether it be funding for systems or ensuring that you have the appropriate staffing levels, provide the resources that will make your cyber program strong.
- Learn from others – stay aware of how other government entities are preventing, mitigating and resolving ransomware attacks.
- Practice your response in advance using tabletop exercises and simulated ransomware attacks. This helps ensure that all leadership and staff are thinking about continuity of operations and contingency plans.
- Talk to other leaders about the importance of having a cyber strategy.
- Be a champion for your government's cyber efforts.

**What to do when your government is attacked**

- DON'T PANIC!
- Be aware of what is taking place. Your constituents may turn to you for answers.
- Let your government's IT professionals and management do their job while you provide support to resolve the current situation.
- Learn from the incident so you and your organization will be better prepared for the next incident.

**To Pay or Not to Pay?**

Stateline.org reports that three states are considering legislation that would ban state and local government agencies from paying ransom if they're attacked by cybercriminals. The intent: Banning payments will deter cybercriminals from targeting government systems. However, some cybersecurity experts have stated that while banning ransom payments is undoubtably well-intentioned, it's a bad idea because local governments, particularly smaller ones, may not be able to restore or rebuild their computer networks quickly. That could prove even far more costly and disruptive than paying a ransom.

The FBI and the US Department of Homeland Security Cybersecurity and Infrastructure Agency discourage paying a ransom in response to an attack but at the same time acknowledge the issues involved.

Today, paying a ransomware demand no longer guarantees your files will be restored at all or in part. The latest data indicates there is an increase in cyber criminals not fulfilling their "promise" to provide kyes to unlock files. Given the growth of cyber-criminal activity they have become careless and slopy in their attacks and in some cases they have failed to restore all files or have unintentionally or not made some files unrecognizable.

**Additional Resources:**

**StopRansomware.gov** website provides cybersecurity resources from across the federal government.

CompTIA – PTI 2020 **National Survey** of Local Government Cybersecurity Programs.

**Protecting Our Data: What Cities Should Know About Cybersecurity** published by PTI and the National League of Cities.