Legal Q&A

By **JJ Rocha**, TML Legislative Liaison

Q. What is cybersecurity?

A. The United States Department of Homeland Security defines cybersecurity as "the protection of computers and computer systems against unauthorized attacks or intrusion."

Q. What is a cyber attack?

A. A cyber attack is a deliberate attempt to gain illegal access to computer information systems, networks, infrastructure, and personal computer devices for the purpose of doing harm. An attack may attempt to steal or hack into a city's system to steal, alter, or destroy information.

Cyber attacks come in different forms. Phishing emails or "social engineering" are one of the most common ways that a system may be compromised. Most people have encountered this type of attack. This type of "malware" tempts a recipient into opening an email by disguising the sender. The sender may look like someone the recipient knows or someone whom the recipient would not be suspicious of but, in reality, it is a cybercriminal attempting to gain access to your files. These types of emails contain a link or attachment that may contain a virus. Even worse, they may contain ransomware that allows the criminal into your system.

Ransomware is a serious threat to governmental entities, private business, and individuals. It is malware that blocks access to your files and system until a ransom is paid by cryptocurrency, e.g. Bitcoin. Depending on the advancement of the malware, it could lead to your system being encrypted making it virtually impossible to access your files, unless a ransom is paid.

Cyber attacks are not limited to those above. There are many ways to infiltrate a computer system including "spyware" and "eavesdropping malware." Other types include man-in-the-middle (MitM) attacks, denial-of-service, structured query language, and zero-day exploits.

Q. Have cities been hacked?

A. Yes. In March 2018, the City of Atlanta was attacked with ransomware. Advanced malware encrypted the city's data and issued a ransom of $51,000 in Bitcoin. More than a third of the City's 424 software programs were affected. Citizens could not pay their utility bills, municipal court files were blocked, legal documents were lost, and police lost dash-cam recordings. However, 9-1-1 services, police, and fire services remained unaffected during the breach. The City of Atlanta has not disclosed much information relating to the breach, but it has denied paying the ransom. (It appears that the attackers lifted the payment portal and left the City to rebuild with lost data.) Atlanta spent over

$2.6 million on emergency operations to handle the initial attack. In order to rebuild their systems and recover information, the information management director requested $9 million more to deal with the aftermath.

The City of Atlanta's ransomware breach is the largest cyber attack on a city to date. In recent years, there have been smaller attacks on governmental entities. In April 2017, the City of Dallas had its emergency siren system hacked resulting in sirens going off for hours. In addition, the City of San Francisco's municipal railway system was hacked in November 2016 by ransomware. The attackers demanded $70,000 in Bitcoin and left the railway unable to collect fares.

Q. Are there any state laws to help protect cities?

A. The 85th legislature tackled cybersecurity for the first time and passed two major pieces of legislation. The Texas Cybercrime Act created criminal offenses for persons who intentionally interrupt or suspend access to a computer system or community network, including by the use of ransomware and unlawful decryption, without the effective consent of the owner. The Texas Cybersecurity Act focuses on network infrastructure and cybersecurity programs for the State of Texas. The Act, effective September 1, 2018, also allows a city to conduct an executive session to deliberate cybersecurity practices (e.g., security assessments, network security information, critical infrastructure, and components of a security system).

Another bill, H.B. 1861, makes any information derived from a city's routine effort to prevent, detect, investigate, or mitigate a computer security incident confidential under the Public Information Act. However, the bill does not relieve a city from consumer notification that may be required by other law.

Q. **What can a city do to protect its systems?**

A. The most important and crucial step for a city to take in protecting its systems is to educate employees on cybersecurity awareness and protect the city's security infrastructure. The United States Department of Commerce's National Institute of Standards and Technology has created a framework to help manage and reduce cybersecurity risk. The framework was first created in 2014 at the direction of the White House and with guidance from private industries, academia, and government. The framework was updated in April 2018.

The Department of Homeland Security has also published a guide for critical infrastructure called "Critical Infrastructure Threat Information Sharing Framework: A Reference Guide for the Critical Infrastructure Community". It describes how threat sharing works in real-life incidents and includes descriptions and contact information for key threat information-sharing entities.

For more information on the above publications and others, visit TML's cybersecurity clearinghouse page at www.tml.org/cybersecurity-clearinghouse.