cyber security

TEXAS CITY ATTORNEYS ASSOCIATION
SUMMER CONFERENCE - JUNE 19-21, 2019

Karen Kennard, Shareholder/Aaron Gregg, Associate
GREENBERG TRAURIG, LLP
300 WEST 6TH STREET
SUITE 2050
AUSTIN, TEXAS 78701
(512) 320-7200

INTRODUCTION

Technology plays a critical role in all organizations and is used in almost every device an organization uses to conduct its business. These devices create, collect and maintain data that is used to carry out the functions of the organization. Cities, like most organizations, have a growing dependence on technology which demands greater measures to insure the security of the data that is created, collected, and maintained by the city. Keeping computer systems, networks, applications, and data safe is what cybersecurity is all about and is a shared responsibility that requires awareness, training, and vigilance. To better understand cybersecurity everyone must become familiar with recognizing the risks, threats, and vulnerabilities posed by unauthorized access to technology systems, networks, applications, and data and develop adequate approaches that address these risks, threats and vulnerabilities

Cities are not immune to the types of cyber threats faced by private companies. In a recently published study, public entities represented 16% of all reported data breaches.[1] The percentage of data breaches experienced by public entities was second only to breaches against small businesses who were reported to be the subject of 43% of all cyber breaches. [2] Much like bank robbery, where the criminals go to "where the money is"; cyber attackers focus on cities because of the rich sources of data and information that cities possess.

Cities create, collect, and maintain voluminous amounts of data and information. As a result, cybersecurity must be a critical focus for cities to protect their information. The ability of city technology systems to communicate among themselves allows large amounts of data to be shared to provide municipal services. The creation of "SMART City" initiatives also creates additional vulnerabilities for cities. The digital transformation of municipal services can make the lives of city residents better; provide more effective consumption of city resources; and create a more efficient governance for cities. Unfortunately, the byproduct of these "SMART" initiatives makes cities more attractive to cyberattacks and other attempts to gain unauthorized access to city data and data systems.

CYBERSECURITY

What is cybersecurity? It is generally believed that cybersecurity is the processes, techniques, methods, and practices used to protect sensitive data, computer systems, networks, applications, and programs against unauthorized access or use that is intended to cause harm or exploitation of data. [3] Implementing cybersecurity measures will generally involve implementation of security methods related to application security, information security, network security and disaster recovery.[4]

CYBERSECURITY RISKS, THREATS, AND VULNERABILITIES

A successful cybersecurity approach has multiple layers of protection spread across the computers, networks, programs, or data that an organization seeks to keep safe. In an

[1]Verizon, 2019 Data Breach Investigations Report
[2]Id.
[3]Digital Guardian, Data Protection 101 – May 2019
[4]Id.

organization, the people, processes, and technology must all complement one another to create an effective defense against cyber-attacks.[5]Cyber risks are now more innovative and sophisticated and better capable of disrupting the security of a city's entire system of technology with the potential to shut down all the city's operations. It is challenging for any organization to overcome these threats and successfully fight back against them. To understand the importance of implementing cybersecurity measures a city must examine the types of risks, threats, and vulnerabilities that they may face. Today most experts believe that effective cyber security protection involves three components: people, processes, and technology.

People. Like all organizations, the most important asset of a city is its people. The employees of a city must be trained to understand and comply with basic data security principles like choosing strong passwords, being wary of attachments in email, and backing up data. The basic cybersecurity principles related to the people in an organization require people in the organization to stop, think, and connect.[6]

Processes. All organizations have processes that are unique to their daily operations. An effective cyber security approach requires cities to develop a plan for how they deal with both attempted and successful cyber-threats. A best practice plan will identify how the organization can identify attacks, protect systems, detect and respond to threats, and recover from successful attacks.

Technology. Technology is essential to giving organizations and individuals the computer security tools needed to protect themselves from cyber-threats. Some of the technology components that a city must include in its cyber security protections include: endpoint devices like computers, smart devices, routers; networks; and the cloud.[7]

CYBER ATTACKS

Cybersecurity risks can emanate from a variety of sources. There are malicious actors who intentionally seek to cause harm to an organization by stealing data and information for money, credit, prestige, or revenge; as well as benign actors who unknowingly or accidentally cause harm by downloading malware on the city's computer network or losing a device containing city data. It is virtually impossible to predict when a cyber threat will occur. The term, cyber-attack covers many activities, but some of the more commonly recognized cyber-attacks include:

- Tampering with computer systems or networks and the data stored within those systems
- Exploitation of technology resources
- Unauthorized access to a computer system or network and the sensitive information contained within the system
- Disrupting normal functioning of an organization and its processes
- Using a computer software to attacks an encrypt the data of an organization[8]

[5]Cisco Systems -Overview of Cyber Security (2019)
[6]U.S. Department of Homeland Security- Cyber Security Guidelines
[7]See, Digital Guardian – Data Protection 101, May 2019
[8]An introduction to Cyber Security for Beginners – GeekFlare, February 24, 2019

A cyber-attack will usually involve a set of consistent characteristics. Those characteristics involve the pattern of the breach, action taken to cause the breach, the asset used to breach. These characteristics may be interchanged to gain access into an organization's, systems, networks, and data.

Actions taken to cause a breach may include the use of malware, hacking, misuse of equipment or data, error, or insider intrusions of an organization that cause a data breach. There are numerous delivery methods that a cyber-attack can take including attacks by email, websites, and mobile devices. Also, different types of cyber-attacks cause different types of harm. Some of the most well-known attacks include the following:

Malware

Malware is a type of software designed to gain unauthorized access to an organization's technology systems and cause damage to those systems. Large government entities with many access points into their technology systems face a challenge in ensuring the breadth of up-to-date malware defenses are implemented to protect the organization from malware attacks. Smaller organizations may lack the budget for malware defenses other than desktop protections. However, basic protections against computer malware viruses can be very helpful in protecting a city's technology systems.

Ransomware

Ransomware is a malicious type of software that involves a file encryption software program that uses a unique encryption algorithm to lock up the files of a target system. The authors of a ransomware attack generate a unique decryption key for each of its victims and save it in a remote server. The creators of a ransomware attack take advantage of the fact that an organization's system is paralyzed and demand a ransom amount from the organization to provide the decryption code to unlock the data. However, paying a ransom does not guarantee that an organization's files will be recovered or the organization's system will be restored.

Phishing

Phishing is a fraudulent action of sending fraudulent emails that resemble or imitate familiar sources by pretending to be sent by a legitimate and reputable source. Phishing mails generally include a strong subject matter line with attachments like an invoice, job offer, or other enticement or offer from a reputable company or an important email from a high-ranking official of an organization. Phishing attacks are the most common cyberattacks that aim to steal a person or organization's most sensitive data.[9]

Theft/Loss/Negligent Disclosure/ Insider Misuse:

A cyber-attack can also be caused by lost or stolen equipment, or data; and misuse of equipment or data by persons with authorized access to an organization's data. It can also be caused by the error of an employee who mistakenly sends data to the wrong person or publishes data on a

[9]An Introduction to Cyber Security Basics for Beginners

public website. Errors in the form of erroneous disclosure of data can cause as much damage to an organization as outsider intrusions into an organization's system.
Insider misuse of data is also a concern that an organization must address to insure the safety of data. An organization can limit the amount of damage an employee acting inappropriately or maliciously can do by reviewing all access privileges that each employee has to the organization's data. Any incident where information or data is compromised, whether through misplacement or malice can cause significant harm.

MUNICIPAL CYBER THREATS

Cities face the same types of cyber threats as private businesses.
In 2018;

- there were 23,399 incidents of cyber-attacks against public sector entities with 330 confirmed attacks that involved a data disclosure;
- Cyber-Espionage, Miscellaneous Errors and Privilege Misuse represented 72% of the attacks with some of the attacks resulting in data breaches;
- External attacks represented (75%), Internal attacks (30%), Partner (external & internal attacks) (1%), Multiple parties (6%) (breaches);
- Espionage (66%), Financial (29%), Other (2%) (breaches).[10]

Studies show that data breaches in the public sector take more time to discover, often taking months and years to be discovered. Public breaches are over 2.5 times more likely to go undiscovered for years. Espionage-related breaches typically take longer to discover due to the lack of external fraud detection. Internal privilege misuse by employees is the most common pattern within public sector breaches that are undiscovered for months or more. Cities must do all that they can to reduce the number of entry points into their organization that a cyber attacker could take advantage to prevent a breach. However, it must be said that even the best cyber security protections can only do so much. A city does not control the development, preparation, targeting, distribution, and other shenanigans that take place on the part of the bad guy who attempts to gain unauthorized access into a city's technology systems However, the city can control how they react to a breach once it happens. There's a great deal that must occur even after the breach takes place to make the breach worth the criminal's while. Preventing access into a city's systems may be difficult, but what data is compromised by unauthorized access can be key component of an effective cyber security plan.

CYBER SECURITY BEST PRACTICES (What to do?)[11]

The increased prevalence of cyber threats requires cities and their employees to take several steps to adopt measures that address cyber-attacks. The fact that everything is connected to the internet increases a city's vulnerability to breaches. There are however some mitigation

[10]See, Verizon 2019 Data Breach Investigations Report
[11]United States Army Command – Principles on How to Protect Against Cyber Threats

steps that can be taken to lessen the impact of these vulnerabilities. Mitigation will involve policies, planning, training and may include some of the following practices:

- Back up data regularly and verify the integrity of those backups regularly. Secure your backups. Make sure backup systems aren't connected to the computers and networks they are backing up.[12]
- Create a solid business continuity plan in the event of a cyber-attack. Create and train cyber response teams within the organization.
- Provide cyber awareness training for employees.
- Be suspicious of unsolicited phone calls, emails or individuals asking about organizational or personal information.
- Submit personal information only to secure, legitimate websites that starts with https.
- Delete emails you think are phishing attacks. Be suspicious of attachments and links contained in emails. Only open emails you are expecting from reliable known sources. If in doubt, "don't open it".
- Test new technology before implementing it.
- Test how your systems may be compromised.

- Ensure security is installed at every possible entry point of the city's technology system and audit security.
- Identify all machines and devices connected to the city's system and assess the defenses that are engaged to protect against unauthorized access.
- Ensure you are utilizing the most up-to-date patches for your software. Implement automatic updates and don't ignore messages to update computers
- Security needs to be multi-layered so that numerous obstacles will be in the way of the intruder.
- Patch operating systems, software, and firmware on digital devices (which may be made easier through a centralized patch management system).
- Ensure antivirus and anti-malware solutions are set to automatically update and conduct regular scans.
- Manage the use of privileged accounts—no users should be assigned administrative access to a city's data unless necessary, and limit the overall use of administrator accounts when necessary.
- Review all access controls, including file, directory, and network share permissions appropriately. If users only need read specific information, they don't need write-access to those files or directories.

TEXAS CYBER SECURITY LAWS

[12]FBI Internet Crime Complaint Center

The 2019 legislative session included the passage of additional laws relating to cyber security. House Bill 64 amended provisions of the Texas emergency management law to include a cyber security event as a type of disaster under emergency management provisions of state law.[13] The bill also amended provision of the Texas Cyber Security Act to require the Texas Department of Information Resources to include local governments in its biannual reports that identify preventive and recovery efforts that the state can take to improve cybersecurity in the state and to include local governments in evaluating programs that provide information security officers to assist small entities in the state.[14] Finally, new legislation will require local governments to identify the most appropriate employees who have access to computer systems and/or databases and require those employees to receive certified cyber security training.[15]

There are also several other laws in Texas that address the issue of cyber security on a broad range of matters.

Texas Nuisance Website Act (Chapter 125, Texas Civil Practices & Remedies Code)

The Texas Nuisance Website Act allows the Texas Attorney General, district, county, or city attorney to bring a lawsuit to declare that a person is operating a website or network that constitutes a common nuisance under provisions of the Texas Civil Practices & Remedies Code. A nuisance of the act can involve activity related to organized crime, compelling prostitution, sexual assault, aggravated sexual assault, continuous sexual abuse of a young child, sex trafficking, or other types of sex crimes.

Texas Cyber Crimes Act (Chapter 33, Texas Penal Code)

The Texas Cyber Crimes Act makes it a criminal offense to engage in certain activities related to cyber-attacks, hacking, and other activities involving computer networks, devices, and digital information. The law provides criminal penalties for denial of service attacks, ransomware, and intentional deceptive data alteration.

Texas Cyber Security Act (Chapter 2054, Texas Government Code)

The Texas Cyber Security Act establishes cyber security requirements for state agencies and includes cyber security as an element of a state agency's sunset review. The law includes the creation of the Texas Cyber Security Council which is made up of representatives of the Governor, Lt. Governor, Speaker of the House, private sector leaders and higher education institutions. The Cyber Security Council, among other things, establishes criteria for addressing cyber threats and provides recommendations to the legislature for legislation necessary to implement appropriate cyber security practices.

[13]HB 64- 86th Texas Legislative Session, amends Chap. 418 TEX. GOV. CODE
[14]TEX. GOV. CODE, Chapter 2054
[15]HB 3834- 86th Texas Legislative Session, amends Section 2054.5191 TEX. GOV. CODE