City of Broken Arrow

Minutes
Special City Council Meeting

City Hall
220 S 1st Street
Broken Arrow OK
74012

Mayor Debra Wimpee
Vice Mayor Christi Gillespie
Council Member Johnnie Parks
Council Member Lisa Ford
Council Member Justin Green

Tuesday, August 20, 2024 **Time 5:00 p.m.** **Council Chambers**

1. Call to Order

Mayor Debra Wimpee called the meeting to order at approximately 5:01 p.m.

2. Roll Call

Present: 5 - Justin Green, Lisa Ford, Johnnie Parks, Christi Gillespie, Debra Wimpee

3. Pledge of Allegiance to the Flag

Council Member Johnnie Parks led the Pledge of Allegiance to the Flag.

4. Public Hearings, Appeals, Presentations, Recognitions, Awards

A. 24-1114 Presentation of Cyber Security Awareness Training for City Council

IT Director Scott Carr reported he would present the Cyber Security Awareness Training to City Council; this training was being given throughout the departments of the City. He briefly reviewed the first few slides which discussed what personal information was, what the PCI (payment card industry) was, HIPPA, and state statute pertaining to governments and governmental subdivisions that own or license computerized data which include personal information (PI) of OK residents. He stated Oklahoma tried to pass the Oklahoma Computer Data Privacy Act which still had not passed fully and without this, Oklahoma ranked amongst the lowest in states in terms of actual privacy laws. He said a federal US Privacy Law was needed. He displayed and discussed slides which reviewed the City's legal liability regarding personal information, what a confidential information breach was, as well as what was safe and secure, and what was not: email, not secure; encrypted mail, secure; Microsoft Teams, secure; OneDrive, secure; SharePoint, secure; network share drive or local computer, secure behind the firewall, but not encrypted and vulnerable to cyber-attacks; outside services like Google, Drop Box, etc., not secure. He displayed and discussed a slide illustrating the City's cyber security architecture and how the City was made safe. He displayed a slide illustrating the City's threat matrix from a cyber security standpoint. He indicated hackers were hunting all City employees and working to access City employee accounts. He discussed who the hackers, or threat actors, were including nation states such as China and Russia. He stated cyber crime was very active and discussed a slide illustrating what the goals and motivations were for threat actors including cybercrime which focused on an individual's information and cyber warfare which focused on weakening, disrupting, and destroying the United States through espionage, international intelligence, weaponization and destabilization. He displayed and discussed a live graphic, a mere fraction of a dashboard of what was happening in real time by one cyber security vendor, which showed attacks back and forth across the world. He stated he had a dashboard which focused on City employees and every minute of every hour it updated City accounts, showing who was trying to hack these accounts, and where these attacks originated. He reported organizations were working diligently to hack into City accounts. He stated hackers, or threat actors, in today's world were militarized actors, militarized units, a part of each country's military, working to hack into other countries. He explained hackers were no longer just individuals, but were large scale businesses, multimillion dollar enterprises.

Vice Mayor Gillespie asked if it was legal in Russia and China to work as a hacker.

Mr. Carr explained all countries had laws against hacking, but if a hacker was working for the military, then it would not be illegal. He stated companies spent a great deal of money on cyber security and counter-hackers. He stated the United Stated had a cyber war which was ongoing and was quite sophisticated. He displayed and discussed a slide which listed governmental ransomware victims. He stated ransomware was the most devastating attack a local government could undergo; it took years sometimes to recover from a ransomware attack and could cost millions of dollars in direct costs alone. He discussed a slide about social engineering, the clever manipulation of the natural human tendency to trust, and how hackers took advantage of this. He discussed the various types of social engineering attacks such as phishing (broad attack), spear phishing (individual attack), whaling (high profile target), etc. He discussed how hackers obtained information about individuals through social

media and phone calls. He warned against giving out information over the phone. He discussed mobile phones and the fact that phones were basically computers. He discussed mobile phone security threats. He discussed riskware which were apps asking broad permissions on a phone which collected information and sold this information to data brokers. He noted GM was being sued for collecting driver data from OnStar and selling this data to brokers. He discussed other lawsuits against data collectors and data brokers who were collecting, selling and buying information. He noted it was legal to collect data through apps on phones because when an individual downloaded an app, permission was granted to collect data, and this data could be anything, including geolocation; certain apps kept track of exactly where a person was at all times. He noted the FTC was suing but might lose because the United Stated did not have a data privacy law in place to say it was wrong to collect and sell this type of data. He discussed Meta data leakage from Facebook, Messenger, Instagram, and WhatsApp who collected precise geolocation data, and could also access the microphone and camera on phones. He stated Meta had partnerships with a host of marketing firms, ad networks, and other entities which collected all data, all the time, in real time. He discussed the type of data Meta could collect from an individual who simply took a Facebook quiz including future information collection. He stated the amount of information which could be collected, and which could continue to be collected, was immense. He stated a threat actor could use Facebook to collect data. He discussed how data collection worked, for example, from an event noting Meta could collect data about the event due to the fact that every person at the event had a mobile phone with at least one Meta app installed; as a result Meta could deduce a person's precise location within 2 feet, record attendees of the gathering, determine common interests, determine conflicting interests, update influence metrics, associate all recent searches, catalog all recent purchases, evaluate purchases made for this gathering, integrate all recent trips taken, calculate topic probabilities, estimate influence probabilities, update shopping metrics, project upcoming destinations, etc. and this could all be done through machine learning, data profiling, probability and statistics, knowledge engineering and geolocation. He stated all of this could be done without accessing microphones or cameras, but most individuals granted permission to microphones and cameras and they could be accessed. He discussed how Meta knew about individual purchases made for an event, who invited who to an event, who was new to a group of friends at an event, who liked whose posts, who recently traveled where, who would likely comment on photos or purchases, and Meta made $100 billion dollars in advertising revenue by using this information. He stated even with all this access and information gathered, Google dwarfed Meta. He explained using the Google search engine, using Chrome, watching YouTube, using any Google app, visiting a website which used Google tracking pixels, etc., all provided Google with information. He noted Google made $279 billion dollars in advertising revenue, and it was all legal. He stated threat actors did not need to do anything illegal to obtain private information, this information could be purchased legally, and threat actors could know anyone's every movement every day, happiest memories, saddest moments, date nights, etc. He said, as such it was very important to know who you were talking to on the phone as it could be someone phishing for information to fill in the last few blanks. He stated the last layer was national security; TikTok was a threat. He displayed and discussed a slide illustrating the TikTok threat timeline: in December 2022 TikTok was banned in Oklahoma for all agencies, employees and contractors of the state; in January 2023, 27 states passed laws banning TikTok; House of Representatives passed a law signed by the President banning TikTok unless it became fully owned by a US company. He reported TikTok executives confirmed the data collected by TikTok was sent to China, and all data collected by Chinese companies were submitted to the Chinese government by law. He stated all Chinese manufacturers were required to install a chip to collect data in computer hardware, and all software manufacturers were required to collect data, and all this data was required to be turned over to the government. He noted TikTok was used in China to control Chinese citizens.

Council Member Lisa Ford asked if the City of Broken Arrow had TikTok in any department.

Mr. Carr responded there was one instance which he approved on a separate device which did not travel. He explained it was approved because on TikTok the Broken Arrow Police Department was getting bashed by a fake account. He stated TikTok would not remove things unless someone was a TikTok user, so one device was approved which did not reflect any City information, and it was not used for anything except for checking TikTok.

Council Member Ford asked if the Police Department posted anything on TikTok.

Mr. Carr explained with one device which was separate from any other device, and did not travel, the Police Department monitored and posted on TikTok to counter some of the lies which were posted about the City of Broken Arrow. He continued with his presentation. He stated unsecured Wi-Fi was a threat as a "sniffer" app could be used to watch an individual's actions while using unsecure Wi-Fi.

Council Member Ford asked if airplane Wi-Fi was secure.

Mr. Carr responded any Wi-Fi which did not have the lock icon was unsecure, even airplane Wi-Fi. He stated another type of threat was network spoofing, where a fake unsecure network was made available, and any individual which connected to the network was then vulnerable to data collection. He discussed phishing attacks (infected emails) versus smishing attacks (infected text messages). He stated there were many other types of attacks. He noted the iPhone was the safest phone, but was certainly not 100% safe, and attacks could be made through a text or phone call, and the only way to clear potential threats was to hard reboot your iPhone. He explained shutting the iPhone off would not clear the memory like a hard reboot, and only a hard reboot could clear out the memory of a threat. He stated Android phones were very prone to exploitation due to the open source operating system. He discussed caller ID spoofing, where caller ID could be faked to imitate a familiar number. He stated cellphones had a feature which always connected to the nearest cell tower, and there were devices which imitated cell towers and collected data when a phone connected.

Mr. Carr discussed potential cyber defense against all these threats including passwords. He recommended the following: use strong lock screen pins, strong passwords, and biometrics; update operating systems regularly; use Mobile Safari Browser instead of apps when possible; avoid public Wi-Fi; disable Bluetooth on Phone when not in use; aways use multi factor authentication on all sites; do not hold sensitive conversations via text or call; for any City business, install and use Microsoft Teams for messaging or calling; do not open attachments or links without verifying through separate and different communication; only use trusted charging cords or accessories, avoid public USB charging stations; perform a hard reboot at least once a week; send any caller not in contacts to voicemail; block every number launching smishing attacks; and block every number which did not leave a voicemail. He explained how to perform a hard reboot on an iPhone.

City Council thanked Mr. Scott Carr for his knowledgeable presentation.

Council Member Ford asked for new contact information cards from Mr. Curtis.

5. Remarks and Inquiries by Governing Body Members

There were no remarks or inquiries by the Governing Body Members.

6. Remarks and Updates by City Manager, including Recognition of Recent Accomplishments by Employees and Elected Officials

There were no remarks or updates by City Manager.

7. Adjournment

The meeting was adjourned at approximately 5:57 p.m.

MOTION: A motion was made by Christi Gillespie, seconded by Lisa Ford.
Move to adjourn
The motion carried by the following vote:

Aye: **5** - Justin Green, Lisa Ford, Johnnie Parks, Christi Gillespie, Debra Wimpee

_____ _____

Mayor City Clerk