LEPC Meeting Minutes
July 11, 2017
12:00 pm Walters State Community College – Foundation Room

The meeting was called to order by Candy Lamb, chairperson of the LEPC. The Pledge of Allegience was lead by Nathan Antrican. Invocation was given by Lt. Billy Gulley.

For old business, Candy introduced LEPC Secretary Lindsey Horn, who made a brief presentation on the survey results from the April LEPC meeting about lessons learned from the Sevier County/Gatlinburg fires.

New business was a handout from the health department regarding Zika. The handout was passed around to all in attendance.

Dr. Eric Powel introduced the speaker, Special Agent Scott Wenger of the FBI. Mr. Wenger began his career as a Special Agent with the FBI in 1996. . In 2003, he was selected to go to the Knoxville Division, where he worked in a liaison capacity at the Department of Energy's Oak Ridge National Laboratory and investigated Foreign Counterintelligence matters. Mr. Wenger has a Bachelor of Science degree in Electrical Engineering from the University of Toledo, a Master's degree in Business Administration from National University, and is a recent graduate from Air Command and Staff College at Air University. Mr. Wenger served as an officer in the United States Air Force from 1988 to 1996 and during that time worked on the design and integration of satellite sensor systems used for strategic missile defense.

Special Agent Wenger thanked the LEPC for asking him to speak. He then gave a presentation regarding cyber security. He began his presentation by defining the jurisdiction the FBI has in terms of criminal and national security. In criminal cases, they have jurisdiction over financial, violent, organized, cyber, public, corruption, civil rights, gangs, and drug related crimes. This authorization comes from Title 18. Under Title 50, they have authority to handle cases of national security such as foreign counterintelligence, counterterrorism, intelligence, and cyber crimes.

He noted that cyber crimes are present in both sections and that cyber crimes happen every day. One example he gave was of Szuhsiung "Allen" Ho, who gave nuclear energy information to China. The maximum sentence he may serve is ten years.

SA Wenger said that many hackers will patiently wait for the right time to strike.

He then gave examples of cyber incidents, such as: Distributed Denial of Service (DDoS), unusual port scanning, ransomware (such as malware, malicious code, and phishing sites). He then went through each of these incidents and explained briefly what they were and what to look for. DDoS, for example, has happened to many banks in recent history. Many of these attacks have major financial impact, which hurt the victim of the attack tremendously.

More incidents he described were Website Defacement, which can cause a company's server to act as a "watering hole" or storehouse of malware, which can then affect others and use your server as a proxy to deflect where the actual attack came from. Unauthorized Access was another example given, and he said the best thing to determine was whether it was done from the inside or the outside of the company.

When it comes to malware or malicious code, it is best to find out the propagation, meaning does the malware spread, replicate, or morph? When ransomware is involved you cannot get your date back unless you keep recent backups of information.

Phishing is another common attack, usually targeting CEO's or other high ups in companies who may have greater access to info, or access to funds. These will usually be a request for money from a source that seems reliable. It is not always directed at individuals who have greater security clearance. SA Wenger recommended using a fake phishing site (phish me) to test employees to see their level of knowledge and awareness of phishing schemes.

At this point a video was played in which talk show host Jimmy Kimmel asked people for their passwords, and many provided the information without realizing it.

The last incident covered was Business Email Compromise. The example was given:
SCOTT@FB1.GOV
SCOTT@FBI.GOV

The top one has a 1 (one) in place of an I (letter i). This is a similar enough account that, at a glance, one may assume they know the person attached to the email, and will be more willing to provide information or funds. Usually, if the FBI is notified within 48 hours, there is a good chance of recovering any lost funds. But report must be made quickly.

SA Wenger then gave a list of steps in a computer crime investigation: First the victim becomes aware of a crime either by themselves or from a witness. They then report the crime to the FBI while collecting best evidence. Best evidence includes: actual compromised hard drive (this is the most helpful), image copy of compromised hard drive, logical copy of affected files, backup of compromised list, contact list, any logs or other investigative info.

To best minimize attacks, it is best to keep logs of all activity, report anything suspicious, have physical and environmental security, control access to information (can have all employees agree they have no right to privacy when using company computer), have two-person accountability system, and ensure procedures to protect network when an employee is terminated. Further steps to take are using complex passwords, DO NOT WRITE PASSWORDS DOWN, don't click on all links sent to you.

The FBI takes no position in a civil suit, but civil suits can run parallel to a criminal case.

Best case scenario for such cases last around 4 months. Worst case can last up to 3+ years.

To report a cyber incident, refer to: www.ic3.gov, iGuardian, and/or Malware Investigator.

At this point Special Agent Wenger opened the floor for questions.

Chairperson Candy Lamb thanked Agent Wenger, then informed the LEPC of the ICS300 training on July 18th and 20th. She then thanked Chick-fil-A for donating lunch and the meeting was adjourned.

The Morristown LEPC would like to thank Chick-fil-A for their generous lunch donation.

Our next scheduled meeting to be held on October 10, 2017.
Topic – Tabletop Discussion: Train Derailment