DELAWARE VALLEY dvrpc REGIONAL PLANNING COMMISSION | Transportation Operations Task Force (TOTF)

Highlights from the July 18th, 2019 Transportation Operations Task Force Meeting

Agenda

1. **Welcome & Introductions**
   Chris King, the Delaware Valley Regional Planning Commission, thanked everyone for attending. Each person in attendance introduced themselves and a number of agencies provided brief reports on recent or upcoming events.

2. **Two Minute Agency Reports**
   DVRPC: Upcoming Events include an I-95 Resiliency Tabletop Scenario Workshop on August 14th at DVRPC. ITSPA Annual Meeting has combined with the PA Automated Vehicle Summit and will take place September 4-6 in Pocono Manor. ITSNJ Annual Meeting to be held on October 28 in Princeton.

   PATCO: As a result of heavy rainfall on June 20th, seven stations were deluged with water and service along the entire line was suspended. Moving forward, PATCO, along with other transportation agencies, must plan for the more common occurrence of severe weather events.

3. **Cybersecurity and Infrastructure Security Agency (CISA), Franco Cappa**
   Franco Cappa, a cybersecurity advisor with the Cybersecurity and Infrastructure Security Agency, a department within Homeland Security, presented on the overall purpose of the agency. As a result of a recent presidential directive, CISA was elevated to 'Agency' status, highlighting the rising importance of cyber and infrastructure security. The goal is for the United State to catch and surpass other nations in cyber capabilities; much like NASA did with space exploration in the 1960's.

   In addition to monitoring and investigating cyber threats nationwide, CISA offers individual auditing for all levels of governmental agencies. They conduct an analysis of an agency's cyber capabilities and defenses and make the necessary recommendations to improve resiliency. Mr. Cappa reviewed a wide-range of threats, as well as provided simple steps individuals and agencies can take to prevent cyber-attacks from being effective.

   To utilize CISA's cyber auditing capabilities, an interested agency should contact Franco Cappa at franco.cappa@hq.dhs.gov.

4. New Jersey Cybersecurity and Communication Integration Cell (NJCCIC)

Krista Valenzuela, a Senior Cyber Threat Intelligence Analyst with NJCCIC, spoke to the day-to-day cyber threats taking place and what can be done to mitigate their effectiveness. Cyber-attacks target common vulnerabilities of both individuals and operating systems and typically fall under one of the following motivators: Nation-state, crime, vandalism, terrorism, or hacktivism. Due to the relatively high-reward, low-risk nature of these acts, cyber-attacks are on the rise across the world.

Social engineering is often used to compromise an individual's credentials (usernames and passwords) for access to sensitive accounts or to convince the user to divert payments to the cyber-criminal. Additionally, ransomware continues to be on the rise. In the event of data being held for ransom, the official position of the government is to not pay. However, the immediate need for the data is often vital for an organization to operate, so in many cases, the ransom is paid, perpetuating the act. At least 1,500 ransomware attacks take place per day, resulting in an average payout of $36,000 (Q2 2019), and causing an estimated $8 billion in damages in 2018.

For those interested in additional information on cyber threats and what an agency can do to mitigate the issue, please contact NJCCIC at NJCCIC@cyber.nj.gov or visit cyber.nj.gov.

5. Artificial Intelligence: History and Workings of Machine Learning

Keith Rayle, a Global Strategist with Fortinet, provided a brief overview on the history and status of Artificial Intelligence (AI). Approaching its one hundredth year of existence, K. Rayle views AI as still in its early stages of development. The first stage consists of AI being able to perform the specific functions it has been 'taught' to do. The second stage is when AI begins to repair itself, and the third stage is when AI has the ability to create other AI. The third stage will take place when quantum computing exponentially increases computing capabilities. When AI reaches its full potential, its impact on the world and society will be extreme. Whether for better or worse is yet to be determined.

In the cybersecurity spectrum, Fortinet has 'taught' its AI to identify and protect against malware. In most cases, malware's code leaves behind a digital fingerprint, one that can be tracked from one system to another. AI is able to search through billions of line of code and identify those associated with previously used malware, rendering the damaging code useless.

6. New Business

- Upcoming Meeting Dates
    - Thursday, October 17, 2019