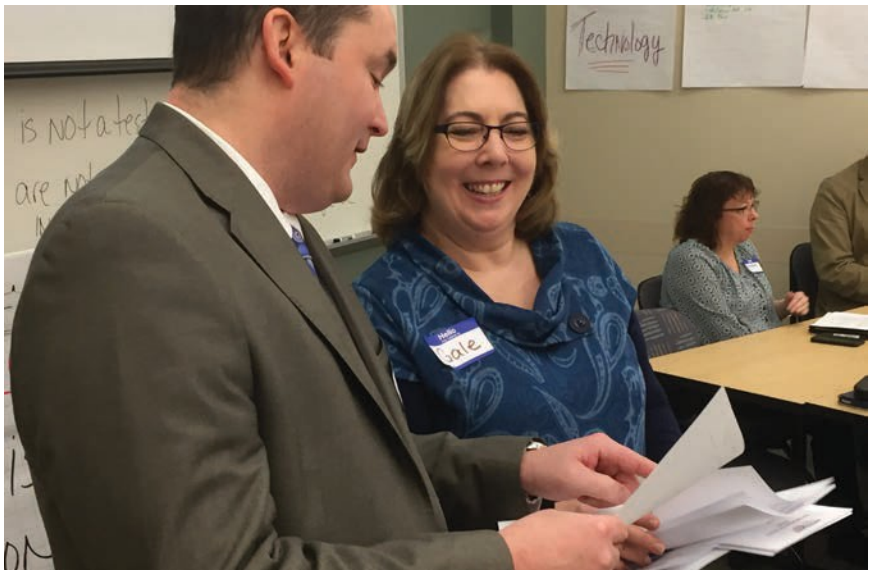
Chapter Focus: Toledo Area Alliance

The Toledo Area Alliance of InfraGard (www.toledoinfragard.org) hosted a Cyber Attack Continuum Tabletop exercise on March 10, 2017, at the Bowling Green State University, Levis Commons campus. Nearly 30 people from various industries participated in gathering and sharing information regarding Cyber Attack preparedness and reactions. This Cyber Attack Continuum was designed to foster an open and highly interactive discussion on the readiness and reaction within and across the following five industries:



- Financial
- Information Technology
- Education
- Retail and Hospitality Facilities
- Healthcare

These industry selections, and the overall design of the Continuum were decided during the initial design discussions. However, the feedback from the meeting suggests that a breakdown of membership industries might have taken this tabletop exercise to a higher level.

The Toledo Area Alliance of InfraGard Board of Directors decided to modify the traditional and publicly provided DHS Tabletop exercises to provide a topic that is relevant to the current membership. After reviewing the available tabletop designs from the DHS websites, we discovered those were outdated, and lacked a current call-to-action scenario. Therefore, we decided

to create our own tabletop exercise, and we formed a design team. Ransomware is a great concern to current industries, and it was decided to build a simulation around this very relevant topic. The design team garnered information from several DHS tabletop exercises and modified the design to fit a ransomware scenario.

The Cyber Attack Continuum Tabletop exercise was opened by the Toledo Area Alliance of InfraGard Chapter President, Lisa Niekamp-Urwin, welcoming everyone in attendance. Board member Kevin Cox then explained how the tabletop exercise will simulate the process of readiness and preparedness. He explained that the group will start by examining what we are doing now to prevent a cyber attack, and then watch a simulated cyber attack video, followed by walking through what we do during a cyber attack, and finally, how do we recover after a cyber attack. Board member and facilitator Gale Lacey explained the tabletop exercise ground rules and led the group through the Cyber Attack Continuum, while former Chapter President Denise Pheils captured photographs — with attendees' permission — and board member Chris Riling provided the simulation video. Finally, board member Brian Schrock and FBI Agent Scott Halbur provided closing remarks and summarized some key findings and information, provided here:

- Vulnerability Management is Crucial
- Law Enforcement — involve them early and often; they are always willing to help
- Testing Incident Response Plans IRP — how many actually do this?
- Backup testing
- Redundant sites — how are we testing?
- Administrative monitoring — user access controls
- List positional roles instead of specific people
- Contingencies — what if the CEO is out of the country?
- Industry standard — 60% of staff is available during an attack
- Internet of Things Monitoring and Securing
- Vendor management
- Vendor list is up to date?
- How you will pay vendors?
- What's the vendor's capacity?
- Consider incident coordination with vendors
- Buddy organizations and equipment as a service
- Sharing information

Policies and Procedures — review and update often

- Financial — consider stock impact/ board impact
- Relevance and Timing — consider how our discussions would have gone if this attack scenario happened 7 years ago, or 3 years ago

One final discussion revolved around paying a ransomware demand. The FBI policy on paying the ransom during a ransomware attack is: "Do not pay." In spite of this official stance, it is commonly understood that businesses may have bitcoin on reserve for emergencies such as this. Bitcoin is usually the form of payment requested. In light of this, a discussion took place pointing out that bitcoin, like cash, is owned by whomever physically holds it. Except bitcoin, unlike cash, is held digitally. If the digital media where the bitcoin is held is compromised, then someone else may now hold, and therefore own, the bitcoin reserves. Also, the nature of bitcoin is its variability. Like stocks, the value of bitcoin varies daily. Therefore, a final recommendation was gleaned, to consider including a trusted bitcoin dealer on emergency response contact lists. While the FBI recommends that the ransom should never be paid, there is some wisdom in knowing and considering every possibility.

This tabletop exercise involved a diverse group of government and industry professionals in an informal setting, discussing simulated situations. This type of exercise is intended to stimulate discussion of various issues regarding a hypothetical situation.
It can be used to assess plans, policies and procedures, or to assess types of systems needed to guide the prevention of, response to, and recovery from a defined event. Tabletops are typically aimed at facilitating understanding of concepts, identifying strengths and shortfalls, and/or achieving a change in attitude. Participants were encouraged to discuss issues in depth and to develop decisions through slow-paced problem solving rather than the rapid, spontaneous decision making that occurs under actual or simulated emergency conditions. (DEMHS, 2017)

References:

National Level Exercise 2012: Cyber Capabilities Tabletop Exercise: https://www.fema.gov/media-library/assets/documents/26845

Ransomware - Anatomy of an Attack, by Cisco: https://www.youtube.com/watch?v=4gR562GW7TI

Vermont Division of Emergency Management and Homeland Security: Templates Needed For Each Exercise Type: http://demhs.vermont.gov/training/exercises/templates