Delaware Cyber Security Advisory Council

Delaware Cyber Security Advisory Council Meeting Minutes
April 27, 2016

Name	Organization	Attendance	Designee in Attendance
Joshua Brechbuehl	City of Newark	Present	
Jason Christman	Delaware National Guard	Present	
James Collins	State of Delaware, DTI	Excused	
Richard Gowen	Verizon	Present	
Mike Maksymow	Beebe Healthcare	Present	
Daniel Meadows	State of Delaware, DSP	Present	
Doug Myers	Exelon Holdings	Present	
Bruce Patrick	Tidewater Utilities	Present	
Marwan Rasamny	Delaware State University	Present	
Diane Rogerson	JP Morgan Chase	Present	
A.J. Schall	State of Delaware, DEMA	Present	
Elayne Starkey	State of Delaware, DTI	Present	

Call to Order

Chief Security Officer (CSO) Elayne Starkey called the second Delaware Cyber Security Advisory Council meeting to order at approximately 9:30 am on April 27, 2016.

Welcome and Introductions

Elayne Starkey welcomed everyone and invited Joshua Brechbuehl to introduce himself, as he was unable to attend the first meeting. The other council members reintroduced themselves. Others in attendance: Claudette Martin-Wus of DTI, OMB Training Administrator Barbara McCleary, Trevor Fulmer from the National Guard, and Lisa Morris and Aleine Porterfield from DOJ. Doug Myers announced Pepco Holdings has changed its name to Exelon Holdings.

Review and Approval of Minutes

Elayne Starkey opened the floor to approve the minutes for both the General and Executive Session of the March 23rd meeting. Elayne explained the minutes for the Executive Session cannot be e-mailed due to confidentiality reasons. Diane Rogerson made the motion to accept the minutes, and Daniel Meadows seconded. The majority approved the minutes for the General Session and the Executive Session, and the minutes for the Executive Session were collected for proper disposal.

Old Business

The trial for eBoard has expired. As we continue to push towards utilizing paperless minutes, DTI is working on finalizing the contract with eBoard for use in the near future.

State Cyber Exercise Program

Delaware's Cyber Security Exercise Program has been up and running since 2005. Planning is underway for the 11th annual exercise this fall. The program has evolved from tabletop only scenarios to functional, hands-on drills using a 3-track system: technical, managerial, and communications/public information. Scenarios have ranged from pandemic attacks and electrical grid attacks to combined cyber and physical attacks. DTI has partnered with many agencies and law enforcement/state police and the National Guard over the years and is interested in including border states in the future. Elayne Starkey welcomes any suggestions for new ideas for the exercises.

DEMA Director Schall gave an overview of the October 2015 exercise. This drill focused on a scenario that escalated quickly and tested how agencies would respond, communicate, and act. DEMA recognizes that any cyber-attack is a public safety issue. Participants experienced real-time threats in the seven-hour exercise. In October 2015, 32 agencies participated and were sent pre-injects, alerts of the practice scenario escalating, 3-4 days prior. There are approximately 150 Continuity of Operations (COOP) plans across the State. These plans must be revisited every year. DEMA sits on the FEMA Region 3 Council, which participates in GridEx, an exercise which focuses on power and utilities and takes place every two years. Doug Myers stated that one of the gaps identified by the GridEx exercises is the ability for Utilities to have their state and federal counterparts participate. The next GridEx exercise is scheduled for November 2017.

Diane Rogerson asked about including the Private Sector in the Cyber Security Exercises. Scenarios of the Private Sector being attacked have been used. Participation/response from banks in the State exercise has been lukewarm.

Mike Maksymow asked if the facilitators have considered multi-day exercises in the future. The closest they have come is using the pre-injects, but it was agreed that a multi-day exercise could make a difference, showing the work it takes to handle shift-changes, communication, and documentation which needs to be done for an event that lasts longer than one day.

Claudette Martin-Wus, the DTI Exercise Director for 2015, discussed the Spear-Phishing component of the exercise. It was designed to educate employees on e-mail scams and to use as a realistic learning tool for State agencies on the impact of clicking links in unsolicited e-mails. During the last exercise, there was a 2.46% click rate by employees who also entered their credentials. After Action Reports recommend that agencies are informed and educated.

Brainstorming and Roadmapping

Barbara McCleary presented the steps the council would take to brainstorm ideas for how CSAC would move forward in its purpose.

The council first wrote down their individual ideas on Post-It™ notes, then broke into small groups to discuss and combined their ideas. In the large group session, they came together to voice their ideas, which were posted for them to organize into categories with headings (see Page 4 for the "Brainstorming and Roadmapping Exercise").

Barbara McCleary will work with Elayne and DTI on the results to create action items and determine what role CSAC can play, including the creation of spinoff subcommittees/workgroups).

FOIA Exemption Proposal

The Freedom of Information Act (FOIA) is designed for the transparency of government operations. It was created before cyber threats began. While physical specifications such as Emergency Response Plans, blueprints, and alarm schematics are exempt from FOIA, computer network designs, source code, and other virtual entities are not. Elayne Starkey expressed a desire to work with the Legislature to add cyber security and Information Technology to the exemption. The exemption would not restrict the release of data; the exemption would protect the underpinnings and technology architecture.

Mike Maksymow said he doesn't feel "CSAC information should be public...anything we say can be taken advantage of by bad actors," meaning cyber criminals.

Following the example of the Governor's Homeland Security Advisory Council, Elayne Starkey recommends a standing Executive Session on the agenda for new threat briefings from the Council members. DAG Lisa Morris stated it can be done as long as the Executive Session remains focused on items exempt from FOIA. A.J. Schall made a motion to draft a letter from the Council on support of this legislation. Daniel Meadows seconded. The majority approved the proposal.

New Business

The Delaware Banking Association has created its own Cyber Advisory Council. Diane Rogerson said the association wants to help CSAC once it is established and would like to know what information to bring to the council.

Delaware State Police is hosting a conference regarding all threats, scheduled to take place in Rehoboth, and a Hometown Security conference in May. They will be looking at what threats are emerging and how they may impact Delaware.

The State Police DIAC is diving deeper into their purpose; where to go, who is needed to accomplish its goals, and investigating what consumers would like to see from a cyber perspective. Many of the ideas also infer new positions, but the State is currently in transition and in a zero-growth state.

The US Cyber Challenge Camp will be held at Delaware State University from July 11th through 15th. The online session to qualify is currently taking place. Anyone can sign up. Scholarships are available for this program.

The Secure Delaware Conference, the annual cyber security workshop hosted by DTI, is scheduled to take place on September 7th at Dover Downs. A call for speakers is forthcoming.

Public Comment

Trevor Fulmer pushed for CSAC's intent to leverage inside resources.

Next Meeting(s)

CSAC discussed the next meeting dates and locations available. All locations must be open to the public. Seasonal traffic was brought into consideration. The next meeting dates are as follows: June 29th, August 31st (pending), September 28th, October 26th, and November 30th. The June 29th meeting may be upstate; Diane Rogerson and Joshua Brechbuehl will check available Newark locations.

The rules of delegating alternates were refreshed for the council. Council members appointed by the Governor by name, not position, are not able to send an alternate to CSAC meetings.

Adjournment

With no further business to be conducted, Daniel Meadows made the motion to adjourn, and A.J. Schall seconded the motion. With no opposition, the motion was carried. The meeting was adjourned at approximately 11:30 am.

Respectfully submitted,
Ronda Ramsburg
Deborah Hawkins

Brainstorming and Roadmapping Exercise

A. Communication
   a. Capability to broadcast alerts and threats
   b. Day-to-day alerts
      i. Login to secure portal
      ii. Directly push out alerts for urgency
   c. Set up a Cyber Security Speakers Bureau for public & business using CSAC members
   d. Make cyber threat information sharing more useful by finding ways to exchange federal, state, and private sector threat intelligence
   e. Set up a Delaware ISAC for information sharing
   f. Identify a state that already has established good communication and open up a dialogue
   g. Sharing lessons learned from cite events (for example cyber lessons learned in New Jersey after Hurricane Sandy)
   h. Improve Social Media (State to local to users)
   i. Influence local and national regulations impacting cyber security standards and policies
   j. Best Practice: know what you have, where it is, and who can reach and fix it
   k. Develop the capacity to share classified cyber intelligence to a cleared group of individuals
   l. Develop a mechanism within the state designated fusion center (DIAC, DE-ISAC) for evaluating and sharing threat information, especially cyber threats to identified consumers

B. Education & Training
   a. Share best practices in preparedness, prevention, response, and recovery
   b. Resources such as college students
   c. Collaboration of talent development and recruiting
   d. Conduct a tabletop exercise within the CSAC
      i. To help drive better situational awareness
      ii. To identify information/communication gaps and opportunities
   e. Identify weak links that could be used to create a state cybersecurity threat
      i. Weaknesses that are not obvious
      ii. Non-state systems that interact with state systems
   f. Include public educational organizations involved in training
   g. Conduct a multi-day cyber exercise among CSAC members and their teams
   h. Conduct more cyber security exercises across industries
      i. Learn effects on one another
      ii. Prevents shut down of offices, doctors, etc.
   i. Sharing generic attack information
      i. Anonymous
      ii. Resolving conflicting agendas (secret vs. publicly known)
   j. Determine which training and exercise events on national and international level apply most to Delaware, then tailor to our needs
   k. ISAC membership/funding for CSAC members
   l. Streamline/refine information sharing as opposed to increasing it

C. Technology Standard & Solutions
   a. Collaboration on improved and integrated Cyber awareness training for Delaware residents
      i. How can we help each other to have a bigger impact?
   b. Standardized Cyber Security Technology across the State with public and private sectors
   c. Mark external e-mails with [E]
   d. Develop best cyber hygiene practices, or circulate existing best practices, to all industry groups/organizations, and government
   e. Separate Networks SCADA vs. Business for stronger security

D. Strategy/Goals
   a. Set goals
   b. Move quickly (Delaware is small and nimble)
   c. Large-scale vs. Stealth (resource availability attack vs. Info gathering)