

The ACSC had a busy first half of 2018 executing across all three of our primary focus areas - collaborative defense, workforce development, and public policy. Our members are active and involved in our workshops, forums and research and contribute critical and compelling insights to our monthly meetings. This information sharing with peers and across multiple sectors provides significant value to our members, particularly through the opportunities discussed below. The success of the ACSC is built on the participation of our member organizations and I thank all of you for your ongoing support.

### Public Policy

In June, the ACSC held a Campaign Cyber Defense Workshop to discuss government's role in election security as well as how to secure campaign operations. Over 80 attendees, spanning industry, education, and public sectors, joined us for this first look at security heading into the 2018 midterm elections. Speakers included Ron Ford, Cybersecurity Advisor (New England), for the U.S. Department of Homeland Security, Cheryl Davis, Managing Director, FTI Consulting and former Director, Cyber Response Policy at the U.S. National Security Council, and Robby Mook, Senior Fellow at the Defending Digital Democracy project at the Harvard Belfer Center,



Hans Olson, Ron Ford, Cheryl Davis and Michael Figueroa

CNN political commentator and strategist and campaign manager for Hillary Clinton. Throughout the day, discussions centered around the under-utilized government resources, two-step authentication & messaging apps as useful tools to prevent hacking. Our afternoon sessions covered reputation attacks, specifically how cheap they are for attacker but expensive for the defender. Joe Trippi, the campaign manager for Sen. Doug Jones (D-AL) gave an in-depth talk about combatting a bot attack. The bot attack cost only \$15,000 but the Jones campaign spent roughly \$1 million to counter-attack its impact.

### Workforce Development

Our Executive Forum roundtable on Cybersecurity Education was held on May 24, 2018 at Northeastern University. We had a robust dialogue between educational program representatives and security executives. Attendees also discussed the early work with the Cyber Education and Training Consortium (CETC), an initiative co-led by the ACSC and the

University of Massachusetts President's Office. The CETC focuses on developing a diverse and sophisticated cybersecurity workforce in New England by connecting educational organizations with the entities that hire their grads. Three areas of potential impact include:

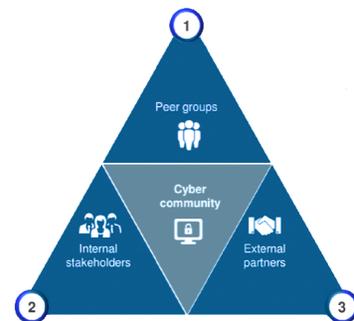
- improving job placement data
- reducing the disconnect between cybersecurity educational programs and industry needs
- and eliminating talent management as barrier to entry

As part of our support for academic-industry partnerships, we are pleased to share a survey opportunity funded by the National Security Agency (NSA). A team of researchers led by ACSC member organization, Northeastern University, is investigating the efficacy of academic-industry partnerships. The more data the cyber security community can gather about what academic programs are offering versus the needs of industry, the easier it is to identify potential opportunities for collaboration. In that spirit, the ACSC asks you for your participation in the study.

All data will be kept confidential. For more information about the study, please read the ACSC blog post which can be found [here](#). To complete the survey directly, please follow this link: [https://neu.co1.qualtrics.com/jfe/form/SV\\_1yQkhlWvlyNCaCV](https://neu.co1.qualtrics.com/jfe/form/SV_1yQkhlWvlyNCaCV)

### Collaborative Defense

Recently the ACSC undertook a project to identify organizational models for efficient collaboration on common defense. Researchers worked with ACSC members and other experts, to interview CISOs, CIOs, analysts, business leaders and others in a range of sectors. Five major areas emerged as opportunities to explore collaboration.



This research gives the ACSC a starting point to build an effective roadmap to improve resilience and communicate our security challenges in our community so we can build stronger defenses together. The report can be accessed on [here](#) on our website.

Our Cyber Tuesdays continue to grow in attendance and we are glad that participants are gleaning useful information. Our next **Cyber Tuesday** is **August 14th**, at the Federal Reserve Bank in Boston, and then **September 11th** at the MITRE offices in Bedford. We hope you'll save the date and join us.

As we look to the second half of 2018, the ACSC is collaborating with the Department of Homeland Security to run a **cyber simulation exercise** with the purpose of developing a

regional-oriented game framework to promote external collaboration among organizations. The date is **September 24**. If your organization is interested in learning more, please let us know.

The next **Executive Forums** will be held on **October 23** and **December 13**. A **Policy Forum** will also take place on **October 3**.

We are also deep into planning our **Annual Conference**, held at the Federal Reserve Bank of Boston on **November 8**. This event is an opportunity for ACSC members and people from the New England cybersecurity community to come together and share information, network, and learn about the latest in cybersecurity. Registration is open for the Annual Conference now and we are expecting a full room of 200 people. **Members can use the code ACSCvip to register for free. Non-Members can use the code EARLYreg for a \$99 registration fee that is closing on September 14th. Click here to [register](#).**

Please visit our website, [www.acscenter.org](http://www.acscenter.org) or follow us on twitter, @ACSCorg to read the latest on what the ACSC is thinking and hearing within the New England security community and beyond.

For more information on membership, please contact Lisa Johnson, Director of Programs and Communications, at [lisa@acscenter.org](mailto:lisa@acscenter.org).

--Michael