From the Executive Director's Desk

When meeting with the ACSC Board ED Search Committee last Fall, I promoted a vision that I called "Enhancing the Cyber Security Foundation for New England." It focused on transforming the organization into a resource that more effectively captures ACSC member experiences to aid the entire community while retaining or even expanding the quality of member engagement. As I finish my first full quarter with the ACSC, I naturally find myself assessing our 2017 progress.

I am pleased to report that our results thus far are very promising. Restructuring our foundational Cyber Tuesday event has received wide approval in ACSC member feedback, with strong engagement and round table conversations amongst front-line cyber defenders drilling deep into several key challenge areas, such as social media phishing response, analytics for security operations, and spam filtering in cloud messaging environments. We also launched the ACSC Collaboration Platform on Slack, a members+friends resource for real-time information sharing, and made final preparations to kick of our Collaborative Cyber Defense study that will detail effective practices in security defense and response across internal groups and external partners.

Our value acceleration will continue into the second quarter. For members, we are launching the quarterly ACSC Executives Forum this month, a premium-level event offered to ACSC member executives, intentionally kept small and intimate to allow participants to share and collaborate rather than be sold. We will kick off a new economic policy study that compares cyber investment opportunity in New England against other regions around the world.

This is just the beginning of a great journey together. I welcome your feedback as we continue our efforts to establish New England as a global hub for cyber security.

Michael Figueroa, Executive Director

By The Numbers

293 - The number of 2016 New England ransomware incidents reported to the FBI.

At the Boston Conference on Cyber Security held at Boston College in March, the FBI reported that "financially-enabled cyber offenses" such as ransomware are growing rapidly.

Thoughts and Trends

Taken from conversations with community members.

"The biggest strength [of ACSC membership] is collaboration and access to the network."

"The new direction is positive and provides a sense of optimism."

"We were able to take stuff [from Cyber Tuesday] and immediately apply it to our environment."

"We're still looking at the equipment and infrastructure as the currency, versus the information."

Policy Focus

The following are some snippets of remarks regarding device encryption, made by FBI Director James Comey during his keynote address at the Boston Conference on Cyber Security, held at Boston College on March 8, 2017. You may see the full transcript of this portion of his speech on LinkedIn: https://www.linkedin.com/pulse/fbi-director-j-comey-device-encryption-michael-figueroa-cissp.

"I want to talk about the impact of ubiquitous strong encryption on our world. And I want to urge you to continue to engage in what is a very complicated and difficult subject.

...In October, November, and December, the FBI received, to our examiners, 2800 devices for which we had lawful authority to open. All them, devices that were seized by state and local law enforcement or by the FBI. 1200 of those devices, about 43%, we could not open with any technique. And these were devices recovered in criminal investigations, gang investigations, pedophile investigations, terrorism investigations, counter-intelligence investigations. With any tool, we could not open 43% of those devices. That is a big deal. And so the question that we have to ask ourselves is, "So what do we want?"

...We all value privacy. I hope we all value security. We should never have to sacrifice one for the other. Our founders struck a bargain that is at the center of this amazing country of ours and has been for over two centuries. And the bargain goes like this: In our great country, all of us, have a reasonable expectation of privacy in our homes, in our cars, in our devices. It is a vital part of being an American. The government cannot invade our privacy without good reason, reviewable in court. That's the heart of America. But it also means then, good reason, reviewable in court, the government, through law enforcement, can invade our private spaces. That's the bargain of ordered good people.

...I love privacy. But I also love and live by the bargain that I talked about that is at the heart of order and liberty. If we are going to move to a place where wide swaths of American life are off limits to judicial authority, that's a different way to live. That is a change of something at the heart of our country, that affects national security cases that the FBI works. It affects criminal cases that the FBI works. It is something that we have to talk about. Maybe it's a good thing, maybe it's a bad thing. But it is not something, in my view, that we should drift. I don't ever want to get to a place where people say to me some day, 'You didn't tell us that the room was going dark in which you operate.'

And so, I'm not going to let that happen. I am keen to force a conversation about this, that people understand the impact so we can have an adult conversation."

Members may get the full audio recording of the speech on the ACSC Collaboration Platform or by email request.