ACSC
Advanced Cyber Security Center
Threat Sharing | Collaborative Defense | Education

ACSC Community Newsletter
Fall 2017

From the Executive Director’s Desk

As the leaves began to turn here in New England, the security community has reeled organizationally from the Equifax data breach and socially from how revelations of sexual harassment and abuse in Hollywood is prompting renewed attention on the subversive hostility women and other underrepresented groups face within the community. The ACSC continues to press for constructive and positive change in these and other areas.

Whereas the media narrative on Equifax centers on the consumer aspects, ACSC members have come together to better understand organizational impact from the breach and what lessons learned they can take away from how Equifax has responded. The ACSC is examining what challenges large enterprises face under similar conditions and how organizations are responding to those challenges today. Through our 2017 *Collaborative Cyber Defense* project, the ACSC is currently wrapping up a study of how large organizations work across internal and external boundaries in defense and response scenarios, identifying effective practices and opportunities for improvement. Our hope is to provide our members with better tools and communications channels to more quickly and effectively handle future major incidents.

Fall also saw the launch of our new diversity-themed research project, *CyberStories: Unlocking the Human Potential of Security*. Launched at the Infosecurity North America conference in October, the focus of our first installments on Women in Infosec takes on new significance as disruption hits on the broader topic around the treatment of women in the workplace. Rather than dwell on the problem space, our hope is to use *CyberStories* to highlight how organizations and the community at large are supporting broader diversity and inclusion to reinforce what works well and emphasize a need to promote collective solutions.

As a community, we have the tools to better collectively overcome the challenges that we face. With the ongoing support of our members and sponsors, the ACSC is working to provide a stronger foundation upon which to use those tools. I look forward to sharing our results with you and working together towards a better community.

Michael Figueroa | Executive Director

By The Numbers

40 / 2 - The number of in-person interviews an ACSC member company conducted against the number of open positions that it was trying to fill.

Thoughts and Trends

Taken from conversations with community members.
“Cybersecurity is a common sport, and we’re all in it.”
“One of the challenges is finding people who want to be a defender.”
“We measure things that are easy, not what is valuable.”

Career Advancement Spotlight: AVP - Secure Payments Initiative | Boston Fed

The Federal Reserve Bank of Boston recently announced two new "executive level" positions that look like great opportunities for experienced professionals looking to step up and leverage their strong identity management and general security backgrounds to be advocates for the next generation in financial payment security in the U.S. The Boston Fed describes the positions as being "executive level" with responsibility for successfully executing Strategy 3 of the Federal Reserve System's Strategies for Improving the U.S. Payments System ("SIPS").

- **Title:** Assistant Vice President - Secure Payments Initiative (LinkedIn Posting with all details)
- **Organization:** Federal Reserve Bank of Boston

We suggest that candidates interested in the position apply directly and let them know that you heard about the position from the ACSC.

ACSC members who would like to amplify key open security positions through ACSC communications may send us the details to info@acscenter.org.

Q&A with Frank Wang

Frank Wang is a PhD student at MIT's Computer Science and Artificial Intelligence Laboratory (CSAIL), with graduate work focused on building secure systems in the PDOS group, where his research interests lie at the intersection of systems, cryptography, and web applications. Frank is also co-founder of the Cybersecurity Factory, a summer program for early stage cybersecurity startups aimed at bridging the gap between academia and industry. Read the full CyberBytes Q&A with Frank on the ACSC web site or download the pdf.

Startup Personality in the Boston Area

ACSC: *What are your thoughts on the startup ecosystem in Boston? How does funding and growing a business in the Boston market compare to other regions like New York, D.C. and San Francisco?*

FW: I think it would be wrong to dismiss the vibrant startup ecosystem in San Francisco, but I think other regions are definitely working hard to play catch-up. Boston has a great ecosystem in my opinion because you have the talent from universities, and a large number of top companies on the enterprise side, such as GE, Akamai, Rapid7, LogMeIn, etc. who have a lot of executive talent. NYC is also great on this front. There is a lot of activity, and they are close to customers.

However, the reason that Cybersecurity Factory has been so successful and popular as a program is that there is really not enough pre-seed/seed funding, especially in security. That's an area that I've heavily focused on and hoping will change. Because of the lack of early funding, you see many fewer first-time entrepreneurs start companies, which is unfortunate. However, I do think this can change with more early-stage funding opportunities. Investors should consider spending more time on the East coast, in my opinion.

What are the benefits to starting a business in Massachusetts? Is there anything we as a community can do better?

Easily, the cost of living and access to talent make starting a business awesome in Massachusetts. That's why some security entrepreneurs spend their whole lives in Boston. However, we don't quite have the vibrant community that other places do, and again, the early stage funding is almost non-existent. Also, the elephant in the room is the non-competes. I think almost all top executives at tech companies agree that we need to get rid of those.

Cybersecurity Startup Trends to Look Out For

In running the MIT security seminar, you're regularly hosting some of the industry's top minds as they look ahead to securing the infrastructure of tomorrow. What are some of the more interesting trends you've discussed this year, and what key takeaways do you have to share with ACSC members?

First and foremost is blockchain innovations. We need more funding and interest to support the hype around blockchains and how systems can be secured by blockchains. People are interested but there is so much going on as people are still trying to figure out what can we really do with Bitcoin and blockchains. The market is inevitable, but still so nascent that everyone is just speculating, and it's very important to have this discussion and collaborate together.

Cybersecurity Innovation Trends

- **Blockchain Innovations**: *"The market is inevitable, but still so nascent that everyone is just speculating..."*
- **Secure Computation**: *"How do we ensure very little information is being stored on the server, or can be leaked from a breach?"*
- **IoT**: *"Until we see a more unified platform...it may not be possible for security companies to secure more than the critical systems leveraging IoT."*

Another area that's really interesting to watch is secure computation. We all have a lot of data stored somewhere in a big data center, and it's going to get breached. So how do we ensure very little information is being stored on the server, or can be leaked from a breach?

This leads to another side, people are thinking more broadly about their data, and about handling/sharing of data. It’s not just stored by one company but data is shared often for fraud prevention and business related activity. How is the privacy of the user being ensured and is it being properly handled as we increasingly gather and share more data?

You also have an interest in building practical, secure systems. What new challenges are introduced by Internet-of-Things (IoT) and other embedded devices as we enable and link intelligent devices to operate within these secure systems?

The problem with the IoT market is that people are building these devices without considering security in the first place. That’s fine, because it’s how new markets emerge. They have very proprietary hardware and no unified network. Until we see a more unified platform in the IoT market, centered around the market-driving players and users, it may not be possible for security companies to secure more than the critical systems leveraging IoT.

Learning From the Equifax Breach

The Equifax breach was a big deal for consumers. It gave us a small window into how consumer personal and financial data is used in the business community while also highlighting how powerless we are at protecting that data. Unlike most past retail data breaches like Target and Home Depot, this one impacts more than consumer credit cards. Those can be replaced with some limited cost. Rather, the data released in the Equifax breach is “permanent” data. We cannot easily change how we identify ourselves. Our names, birth dates, family associations, past residences, and social security numbers cannot be changed. All the data that forms the basis of legal residency, privilege to vote, ability to be employed, right to drive, and many other aspects of our lives is contained in the records that that Equifax and the other credit bureaus hold...*continue reading online in ACSC’s new Perspectives series.*

Recommended Reading

Boston Globe, September 8, 2017: Have you been hacked? What to do after the Equifax data theft
CyberWire, September 12, 2017: The Equifax breach: preparations and incident response
Mass.gov, September 13, 2017: Baker-Polito Administration Announces New Cybersecurity Center At Mass Tech Collaborative
Healthcare IT News, September 13, 2017: Cybersecurity is hard, got it? But let's stop blaming hospitals for every breach
Infosecurity Magazine, September 14, 2017: The Battle for Cybersecurity Talent in America: East Coast vs. West Coast
University of Massachusetts, September 14, 2017: UMass and Advanced Cyber Security Center launch Cybersecurity Education and Training Consortium
Connected Care Watch, September 18, 2017: A clarion call for healthcare security collaboration
Boston Herald, October 5, 2017: Push is on to get new form of ID
MIT Technology Review, October 30, 2017: A Lack of Cybersecurity Talent Is Driving Companies to Use AI against Online Attacks