From the Executive Director's Desk

The vulnerability gremlins wished us all a Happy New Year with the Meltdown and Spectre disclosure from Google on January 2. While the disclosure came a week earlier than the industry planned following a public release, the industry-wide efforts following the initial vulnerability report in June was commendable, likely representing the most successful example of collaborative cyber defense to date. Over six months, dozens of chip manufacturers, operating system companies, browser developers, and cloud services providers worked together to lay the foundation for maintaining public trust in their operational integrity. I, for one, applaud their efforts.

However, the disclosure revealed serious response deficiencies. The early disclosure appears to be rooted in two failures of response discipline. One, a suspect Linux kernel patch just a day immediately following a kernel update sparked community-wide speculation that elicited heightened inspection. Two, an AMD engineer inadvertently noted the root cause architectural function at the heart of the vulnerabilities when responding to the Linux patch in a blog post, essentially painting a target on the problem space. The initial response also failed to go beyond "tier 1" system and service providers, relying on a network on already established peer-to-peer relationships versus any organized response. This provided a competitive benefit to organizations "in the know" and left other critical organizations, scrambling to respond after the public disclosure. Since the disclosure, we have been faced with competing guidance, misinformation, and broken software patches...despite six months of preparation.

Challenges in response aside, Meltdown and Spectre represent a case study in how security information sharing is evolving. The pervasive interconnectedness of the digital economy and the technology supply chain that powers it disallows any one organization from solving big problems on its own. Rather, organizations need to establish new collaborative defense models to overcome the obstacles. I look forward to working with ACSC members and the New England security community at large to build more effective collaborative practices that will provide the foundation for the next generation information sharing relationships.

Michael Figueroa | Executive Director

By The Numbers

68% - The percentage of MA consumers that reported being unlikely to continue doing business with a company that breaches personal data.

Thoughts and Trends

Taken from conversations with community members.

"The more a company goes to a cloud environment, the harder it is for the CIO to attract talent."

"There needs to be more information and knowledge sharing, then focus on talent."

Career Advancement Spotlight: Cyber Security Manager | MIT Lincoln Laboratory

MIT Lincoln Laboratory in Lexington, MA, recently announced a new security operations management position that looks like a great opportunity for a strong security practitioner that has some management experience and is looking for the next step towards an executive leadership position. Reporting to the Deputy CIO for Technology and Infrastructure, the Cyber Security Manager is described as providing "leadership, direction and is responsible for the execution of strategic and operational plans for the cyber security functions. Located along side Hanscom AFB, MIT Lincoln Laboratory has a national security mission that requires sophisticated internal security functions.

- **Title:** Cyber Security Manager (Direct Posting)
- **Organization:** MIT Lincoln Laboratory

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

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

Cyber Security Post Equifax

After going through the initial fall-out from the Equifax data breach last Fall, the ACSC commissioned a survey of Massachusetts residents to better understand public opinion on consumer and privacy matters as well as the perception of cyber security in relation to internet usage. Released in December 2017, key findings in the report include:

- **MA Residents do not believe they are threatened**. Despite the reported widespread impact of the Equifax breach, 49% of MA residents say they did not believe they were affected by it, with another 30% not sure. Only 22% reported they were affected.
- **Privacy Costs**. While close to 70% of respondents say they would be not likely to continue to do business with an organization that suffers a security breach and releases personal data (48% "not very likely" and 20% "not likely at all"), still 29% of residents are "somewhat likely" to continue doing business with an organization after a breach of this kind.
- **Concerns About Data Privacy Remain High**. An increasing majority see the benefits of the internet and technology outweighing privacy concerns. Some 53% of respondents report that the privacy of their personal information is a major concern, up from 39% in 2015; 89% overall report it is either a concern or major concern, up from 75% in 2015
- **Internet More a Benefit than a Threat**. At the same time, nearly 2/3 of those surveyed believe the internet has more benefits than threats to privacy, up from 56% in 2000 as internet usage has become part of daily life and over 90% report they have made an internet purchase in the last six months. Close to 80% now support the advantages of

computerized medical records as worth the tradeoff in privacy risks, while less than 50% thought they should be encouraged in 2000.

- **Federal Government Needs to Lead**. 92% of residents agreed with a statement that the federal government should set tougher data protection standards for technology and data companies. However, nearly half of residents report they have never taken action to protect personal credit information, including enrolling in a credit monitoring program or putting a freeze on credit reports.

Save the Date!

The **2018 ACSC Annual Conference** is scheduled for November 8, 2018 at the Federal Reserve Bank of Boston. We are in the early planning stages and hope to get more information out soon.

Be on the lookout for more exciting event announcements soon!

- **Confusion and Lack of Awareness of How Consumer Data Is Used**. Residents generally are far more comfortable with firms using their data to market to them more effectively than they are with finance firms sharing or selling their credit data. Credit data sharing raises almost as much concern as the risks of unauthorized use of medical records.
- **Unsure of Consent Models**. 48% of residents say giving consumers the choice to opt-out of sharing data is better for consumers, and 52% believing opt-in is better for consumers. This underscores a level of public confusion and the need for better public information and easier tools for consumers to use to take charge of their personal privacy.

One interesting take-away relates to that last point. Security and privacy experts generally believe that opt-in is the most effective model for giving consumers the control they desire over the distribution of their personal information. Consumer responses that align with those experts tend to be more highly educated, with 56% of undergraduate degree holders and 62% of post-graduate degree holders favoring the opt-in model. In contrast, 68% of MA consumers that finished their education with a high school diploma and 56% of those that completed some college without receiving a degree favor opt-out models. This may suggest a socio-economic disparity in how people are able to protect their personal and financial information that warrants further investigation.

Read the announcement and download the full report from the ACSC web site.

Recommended Reading

SClibrary, January 4th, 2018: The Picture of Threat Intelligence (Michael Figueroa contributed)
Xconomy.com, January 16th, 2018: AI Could be Double-Edged Sword for Cybersecurity Industry in 2018
Ars Technica, January 17th, 2018: The impromptu Slack war room where 'Net companies unite to fight Spectre-Meltdown.
Board Effect, January 24th, 2018: Why Cybersecurity Requirements Are Growing for Board Members
BostInno.com, January 30th, 2018: Top Boston Tech Hires, Promotions In January (Lisa Johnson mentioned)
Michael Figueroa, Background on Meltdown/Spectre root cause architectural issues (2016): Reboot Computer Security for IoT

Cyber Tuesday Recap

The Cyber Tuesday for January 2018 focused on two areas of discussion. First, we discussed workplace initiatives for vocational training of cybersecurity professionals as well as cybersecurity degrees from higher education. Then, we discussed the first steps defending against the Meltdown/Spectre threat.

Retraining as a Strategy for Security Workforce Development

Renier Moquete, CEO of advoqt, and Carol Roby, Executive Director of advoqt's Cyber Warrior Academy initiative, discussed their approach to building an intensive 10-week cyber security training program in the Boston area. Designed to take lower level IT professionals, such as help desk personnel, and prepare them for entry-level security analyst positions, Cyber Warrior academy aims to make security careers more accessible to people who did not necessarily gain core security skills through other education pursuits. In a round-table conversation, the Cyber Tuesday discussion focused on a several key questions, including:

- What is more important for cyber security professionals right now, vocational training such as a certificate, or a more advanced bachelor's or master's degree?
- How can organizations reach out to the local higher education community to help design curriculum so they can ensure graduates are ready to work?
- Is there a way to streamline engagement between recent graduates and employers looking to hire?
- How can the higher education community work together to create effective programs that support the overall local cyber security community?
- How can the higher education community work with local employers to help find instructors willing and able to teach the classes?

Cyber Education and Training Consortium (CETC) Update

The ACSC and the University of Massachusetts convened the inaugural CETC meeting on December 8, 2017. With nearly 50 senior and executive participants representing over two dozen local higher education institutions, the meeting exceeded our initial expectations and demonstrated how hungry the New England academic community is to help open the cyber security education flood gates and channel new talent into the local ecosystem. Some key takeaways from the discussion include:

- Current curriculum seems to be balanced between "Blue" team defensive skills and "Red" team security research skills. This may be in conflict with industry needs that vastly favor the former over the latter.
- Nearly ⅔ of respondents reported Average to Poor industry engagement with their institutions programs.
- Institutions are generally comfortable building programs. They are struggling to overcome a supply gap of experienced instructors willing to commit their time while interested qualified professionals feel overwhelmed by a lack of resources to aid them in preparing to teach.

Many of these questions also are being discussed at the higher education level through the Cyber Security Education and Training Consortium (CETC) led by the ACSC and the University of Massachusetts. One key ACSC objective for 2018 is to explore the effective practices in the area and develop a stronger feedback channel between industry and education community to enhance the New England cyber security talent channel.

Meltdown and Spectre Vulnerability Disclosure and Response

January security activities were dominated by the industry-wide response to the Meltdown and Spectre vulnerabilities. The Cyber Tuesday round-table focused a great deal of attention on how ACSC members initially responded to the disclosure and what the vulnerabilities would mean for the long term. Some key areas of discussion included:

Upcoming Meetings

- **CETC**: Thursday, February 8 - Boston *(contact us if you would like to attend)*
- **Cyber Tuesday**: Tuesday, February 13 - Boston Fed, featuring a briefing from the Northeastern Global Resilience Institute on secure information sharing.

- Patching is important, but members expressed some wariness that some patches are "breaking" some software platforms and causing problems. Initial recommendations from the vendor community were to "patch first, test later." However, since Cyber Tuesday, member wariness proved warranted when many vendors rolled-back updates due to a bad microcode update provided by Intel.
- Executing a risk assessment within the organization for critical systems that need additional monitoring will be crucial. While the only effective way to correct the vulnerabilities will be to replace hardware, members conceded that hardware replacement will be a long-term correction that will not happen immediately. Rather, to properly prepare and prioritize, organizations should identify those systems most at risk and plan to replace that hardware earlier than they normally would once the appropriate connections have been made in the supply chain.
- While some reports of a virus exploiting the Spectre vulnerability appeared leading up to Cyber Tuesday, nothing has yet proven to be widely exploiting to date. This suggests early thinking that the vulnerabilities would be difficult to exploit in the wild was correct, giving organizations some time to implement layered defenses against exploitation.
- Cyber Tuesday participants agreed it's best to keep a steady focus on chip manufacturer road maps to know when hardware level corrections will enter the supply chain. It's unlikely the manufacturers will change existing road maps substantially given the length of new chip design processes, so organizations should expect to have to live with the vulnerabilities for some time.