From the Executive Director's Desk

Imagine for a moment the mentality of a ransomware attacker. Much of the effort that goes into conducting a successful attack occurs in preparation. The attacker must develop or purchase the code for the malware package. Botnet services and distribution channels must be procured. To ease the pain of collecting payment and managing unsophisticated users, perhaps the attacker procures underground payment processing and customer service support. However its evolution, a successful attack starts with an investment in time and money.

Once the attack commences, targeted organizations suffer the consequences. Whether they absorb the attack or pay the ransom, the targets have the choice of whether to share information about the attack with other organizations. Typically, they refrain from doing so to stave the potential reputation damage and most certain sense of embarrassment. But, when they make that decision, the attacker gains a higher return on investment through either payment or lessons learned without any significant downside. The non-sharing organization essentially dilutes the attacker's initial investment by empowering additional attacks with little added friction. The result shifts the economic advantage in favor of the attacker.

Cyber information sharing is hard. While our adversaries have mastered it, often work collectively towards common cause objectives, legitimate organizations continue to work in isolation. But, by building trustworthy sharing relationships, we can add cost to subsequent attacks, thereby regaining the economic balance that we need to strengthen our community. The ACSC is implementing the programming and conducting the research that raise the baseline for those relationships in New England. I look forward to continuing our work with you as we work to overcome the adversity.

Michael Figueroa, Executive Director

By The Numbers

41% / 28% - Of 2016 incidents reported to the FBI Cyber Division, the percentage of damages caused by insiders compared to the percentage of reported incidents that were categorized as insider attacks.

Thoughts and Trends

Taken from conversations with community members.

"[Cloud Providers] just don't have the ability to engage customers."

"University curriculum is based more in the needs of the involved faculty than the needs of the learners."

"We have to understand that we won't be able to keep everyone out."

"It's so hard to get a timely response [from cloud revive providers]."

"We need to begin stating what the [security] ecosystem is and building strength in execution."

Kasha Gauthier Appointed Director in Residence for Community Engagement

In her new role, Gauthier will focus on demystifying the cyber security career pathway in order to help security practitioners, professionals, and executives overcome the challenges they face as they advance in their careers.

"Kasha Gauthier is an established leader in the New England cyber security community who brings to the ACSC a strong perspective on what it is to conduct the business of security well," said Michael Figueroa, Executive Director of the Advanced Cyber Security Center. "The ACSC has moved beyond threat sharing to provide members with substantive analysis that helps them build more effective security teams. Kasha brings the proven experience and leadership necessary to spearhead ACSC initiatives that help channel talent into local jobs, encourage collaboration, and make New England a global hub for cyber security."

"I'm thrilled to be working with the ACSC, advancing the organization's mission of strengthening our Infosec community here in the Northeast," said Kasha Gauthier. "Given the cyber security challenges ahead of us, now more than ever is the time for industry, government and educational sectors to work together."

Gauthier brings 15 years of leadership experience to the ACSC, having held a range of strategic positions at organizations ranging from startups to Fortune 100 companies. Most recently Gauthier was CFO/COO at Pwnie Express, an Infosec startup focused on IOT threats.

View the full announcement here.

Engagement Opportunities

We are expanding the **ACSC Counsels' Policy Forum** to include New England law firms! Already viewed as a resource for providing expertise on public policy efforts, this group meets quarterly to discuss legislative and regulatory initiatives, their potential impacts, and how the ACSC can best respond. **Our next meeting is 12-1:30 PM on July 18.** Please contact us for more information about how to get involved.

ACSC in the Community

5/10/2017: "Is a Hybrid Cloud Strategy Safe and Scaleable Enough For Our Industry?" - FIMA 2017

5/12/2017: "Countering Advanced Cyber Threats with a Stronger Community Defense" - KRI Cyber Conference

5/15/2017: "What the ransomware attack means for Massachusetts businesses" - Boston Business Journal

5/16/2017: "Cyberattack could cost billions, but so far US has been mostly spared" - Boston Globe

Communicating with your Cloud Providers - Feast or Famine?

When we talk about collaboration, we often talk abstractly about our needs: how we NEED TO WORK individually with other team members, how we NEED TO ENGAGE with other departments, how we NEED TO SHARE intelligence with our business partners. However, collaboration in practice rarely fits with our abstract perception of need. Instead, when security professionals discuss how we actually engage in collaborative conversations, we tend to steer away from formalized organizational relationships towards more personal one-on-one relationships. As the business partners and service providers that organizations engage continue to diversify and multiply, security professionals face the reality that, in practice, the number of personal relationships we need to maintain to effectively defend assets under our purview are similarly multiplying and diversifying.

Managing security in modern cloud-enabled architectures is a very complex endeavor that requires a different set of skills and prioritization than does internal infrastructure management. With cloud services providers, executives lose control not only over how the services are provided, but over what information they are able to receive. Security executives have generally bought in to the idea that the service providers can better protect the organization's assets and functions, but that does not mean that they trust their providers. In practice, executives and their staff members are unable to credibly verify that the services they receive meet security requirements, a necessary capability to maintain a perception of trust in their providers. What is worse is that the the providers seem disinterested in changing that perception, assuming that organizations will stick with them despite misgivings simply because of inertia, the fact that changing from one provider to another is hard.

New England Cyber Security Update (Curated by ACSC Intern Jordan Kaplan)

- CyberArk acquired Conjur (Newton, MA) for $42 Million ($2.63M in Total Funding)
- Microsoft acquired Hexadite (Boston, MA) for $100 Million ($10.5M in Total Funding)
- CounterTack (Waltham, MA) receives $20M in Series D funding ($98M in Total Funding)
- MIT receives $1.5M from Internet Policy Research Initiative for early-stage Internet policy and cyber security research projects.
- "The Behavioral Economics of Why Executives Underinvest in Cybersecurity" (HBR)

Send your updates to Jordan (jkaplan@acscenter.org) to be included in the next ACSC Newsletter.

That the trust between executive customers and their cloud providers is tenuous presents a real threat to the established providers and an opportunity for disruption. In the first push to adopt cloud services, organizations were motivated by the perception of significant cost savings and the ability to relinquish the pain of managing the associated infrastructure. But, as adoption reaches saturation, the importance of perceived savings will diminish and be replaced by the need to more tightly integrate the services into the organization's security workflow and architecture. Those cloud providers that provide greater transparency and collaborative access will be best positioned to weather that perspective shift.

The ACSC suggests three key enhancements for cloud services providers to become more friendly to the next generation secure organizations. They include:

1. Engaging in Active Security Information Sharing

Cyber defenders want more regular information from their cloud services about how provider internal security operations are functioning. Understanding more about what threats the providers are actively facing, how they are mitigating those threats, how they have responded to attacks, and their road maps for enhancing security capabilities is critical for building a stronger trust relationship between the providers and their customers.

2. Choosing Control over Allowance

Providers that deploy functions and capabilities that cater to the needs of the security and business executives who pay the bills versus the employees who bypass procurement controls to acquire service will likely establish a much stronger and sustainable overall relationship.

3. Establishing Active Communications

Cloud service providers generally only make account managers available as direct interfaces to their customers. Those providers that assign dedicated technical and security support representatives to their accounts will likely find much stronger customer attachment, especially with more sophisticated organizations that have strong security operations capabilities and engaged security executives.

Read the full article here.

Upcoming ACSC Events

July 11: **Cyber Tuesday** - Hosted at the Federal Reserve Bank of Boston. Planned content includes a reverse engineering briefing from Senrio.

July 12: Executives' Forum - Hosted at Veracode in Burlington. Planned content includes round-table discussions on DevOps and IoT.

July 18: Counsels' Forum - Hosted at Foley Hoag in Boston. Planned content includes determining the 2017 agenda and discussing device encryption.