From the Executive Director's Desk

I often hear a lot of personal experiences and how they govern security decision making. In some respects, the security community is founded on what we have learned from doing. Something goes wrong, we examine the symptoms, diagnose the problem, and then implement some corrective action based on our analysis. If the response works, we repeat it. Otherwise, we throw it away and try something new. Whatever the result, we are very willing to share it with our trusted networks and may even share the information in social media and/or at conferences, if it is not too embarrassing.

While sharing experiences is critical for building a stronger community defense, depending too much on the actions of the individuals around us impedes our ability to collectively grow in other ways. This showed throughout the second quarter of 2017 as the ACSC focused our conversation on cloud security. For example, ask security professionals what they do to protect their cloud surfaces, they will talk about the tools they use, what services they subscribe to, and how they work with their providers. But, ask what the cloud security ecosystem looks like, and every one of us will give a different answer. Our global security model is based more on our individual perceptions of what is available and in use than a comprehensive understanding of the market space. Because we lack standard references from which to baseline our conversations, the conversations stay ever fluid and condemned to conditions of constant change that neither scale broadly nor allow for sustainable defenses.

The ACSC continues to work on establishing a stronger baseline for cyber security by developing more foundational resources that provide the references needed to build more consistent defenses. Through intern projects focused on defining a baseline cloud security ecosystem to projects aimed at better understanding how new startups represent indicators of how the ecosystem will change in the future, we are building the models that the community needs to be more effective in countering the attacks that we face today as well preparing for the advanced threats that we will face tomorrow.

Michael Figueroa, Executive Director

By The Numbers

86 / 49% - Number of MA cyber security startups with less than 50 employees against the percentage of those companies that have received private investment.

Thoughts and Trends

Taken from conversations with community members.

"Cyber should not fundamentally be the responsibility of the users using the technology."

"Identifying the space and identifying the consequences is a necessary first step [for considering active defense strategies]."

The Problem that We're Trying to Solve

The following is adapted from a recent blog posting. You may read the full article here.

All security professionals can point to examples of a common story. On a conference room white board, along with all of the notes about organizational strategy around some initiative, there is a box drawn in the upper right-hand corner with the ubiquitous "Do Not Erase" instruction. Inside is a username and password. While the target of that information was not clear in the note, even non-security professionals could rightly assume that the information pertained to the computer resident in the conference room.

Writing authentication details for a conference room computer does not represent a high risk. Chances are, the credentials map to a local account with limited network privileges, and the people who would see it are generally trustworthy enough to be allowed in the office space. The business risk is minor versus divulging domain credentials on a dark web forum to seek help in assessing a threat. We accept little risks in every day life and generally suffer no damage as a result. People do not put credentials on white boards because of ignorance. They do so because they choose to. Similarly, administrators protect sensitive credentials because they understand the impact potential of divulging them and choose control over convenience. By belittling risk-based decision-making as poor hygiene or a failure of security awareness training, security professionals undermine their credibility as business enablers.

From the business management perspective, the problem that security professionals are trying to solve is the community's lack of maturity demonstrated through our skewed perspective with regards to business decision-making. Security folks need to come to terms with the fact that risk acceptance means accepting limited damage to better enable the flow of business. They need to understand their roles as business enablers so that they can improve how they communicate with executive peers and board directors. They need to collaborate better on what is working well and what isn't so that they can stop repeating each other's mistakes. They need to find new ways to measure success rather than only measure failure. And, when things go wrong, they need to examine the root cause and correct when necessary, without judgment.

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.