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

From the Executive Director's Desk

I have had the privilege of speaking with dozens of ACSC participants and community members since coming on board in late November. I am impressed by the high level of optimism represented community-wide. Despite the challenges that we collectively face, our community deeply believes that we have and will continue to overcome those challenges. The threat environment can be daunting, but we thrive on the adversity that we face every day.

What is also clear is that we cannot continue to do it alone. Despite facing common threats, organizations tend to defend against them individually. The lost productivity stemming from the duplicative commitment of resources is likely staggering. As the asymmetry of cyber security increasingly favors the attacker over the defender, we face a new reality where the efforts of any single organization are out-matched by the increasing sophistication of adversarial capabilities.

In 2017, the ACSC will help level the playing field by establishing the foundation for a new community defense approach. Extending beyond our threat sharing and collaboration strengths, the ACSC will press into new strategic areas. We will explore how the business of security is altering executive decision-making, document case studies that highlight what works and what does not work in the modern security ecosystem, examine career pathways for growing and strengthening our workforce, and engage public officials to promote more informed policy decisions.

I look forward to working with the entire community as we continue this journey together.

Michael Figueroa, Executive Director

By The Numbers

1:200 - The ratio of security staff to other staff in one organization.

In a brief survey of security professionals, responses to a question about what they would recommend is the ideal ratio of security staff to other staff ranged from 1:50 to 1:2000. Where does your organization fall? Please let us know.

Thoughts and Trends

Taken from conversations with community members.

"The information sharing and face-to-face aspects [of participating in the ACSC] are the most important."

"Finding new talent is probably our biggest pain point."

"I have a good channel to talent, so my concern is how to give my people what they want to retain them."

"Folks may be really surprised by the really bad stuff out there."

"How do we leverage tools that we already have in different ways?"

Ecosystem Focus

Organizations are beginning to leverage a variety of new collaborative work tools to provide more effective ways to share information and results in real time with their coworkers. The cyber security community has broadly latched on to the tools for a variety of uses that extend both within and outside of their organizations. Because these services represent an important new component of the advanced cyber security ecosystem, the ACSC conducted a high-level survey of the leading tools. The table below shows our initial results.

ACSC Collaborative Work Tool Feature Survey

	Interfaces			Features					Infrastructure				User Administration					Encryption			Access				
	Web Browser	Desktop App	Mobile App	Native Voice Chat	Native Video Chat	File Sharing	Screen Sharing	App Integration	Public Hosted	Enterprise Hosted	Internal Server	Storage	Unlimited Users	Guest Access	Custom Groups	Strong Auth	Credential Sync	Transport	Data-at-Rest	End-to-End	Open Ecosystem	Archive Search	Data Export	Data Retention	Customer-only
ClearChat	✗	⊘	✗	✗	✗	✓	✗	✗	✓	✗	✗	⊘	✓	✗	✗	✗	✗	✓	✓	✓	✗	✗	✓	✓	✓
Google Groups	✓	✗	✗	✗	✗	✓	✗	✓	✓	✗	✓	✓	✓	✗	✓	✓	✓+	✓	✓	✗	✗	✓	✓	✓	✗
Atlassian HipChat	✓	✓	⊘	✓	✓	✓	✓+	✓	✓	✓	✓	⊘	✓	✓	✗	✗	✓+	✓	✗	✗	✓	⊘	✓	✓+	✗
SpiderOak Semaphor	✗	⊘	⊘	✗	✗	✓	✗	✗	✓	✓	✗	⊘	✓	✗	✗	✓	✓+	✓	✓	✓	✗	⊘	✗	✗	✓
Slack	✓	⊘	⊘	✓	✓	✓	✗	✓	⊘	✗	✗	⊘	✓	✓+	✓+	✓	✓+	✓	✓	✗	✓	⊘	✓	✓+	✗
Symphony	✓	✓+	⊘	✗	✗	✓	✗	✓	✓	✗	✗	⊘	✓	✗	✗	✗	✓+	✓	✓	✗	✗	✓	✓	✓+	⊘
Microsoft Teams	✓	⊘	✓	✗	✗	✓	✓	✓	✓	✗	✓	✓	✓	✓	✓	✓	✓	✓	✓	✗	✗	✓	✗	✓	✗

Key

Symbol	Meaning
✓	Available Feature
✓+	Optional Feature
⊘	Partial Feature
✗	Unavailable

The table above shows that two solutions came out on top with regard to available features, HipChat and Slack. In our initial assessment, Slack is stronger at providing collaboration beyond organizational boundaries versus HipChat which targets more internal enterprise activities. Services from major vendors tended to require some level of ecosystem attachment, with either a free Google account or G Suite subscription needed for Groups or an Office 365 subscription for Microsoft Teams. Other emerging vendors provided more limited feature support (ClearChat and Semaphore) or were targeted to a specific market sector (Symphony focuses on Financial Services).

We noted two trends to consider. First, end-to-end encryption disallows external inspection, but also constrains what interfaces can be available (no web browsers) and prevents data retention. Second, native group management options are severely limited. Both trends have enterprise implications.

Despite security concerns, Slack seems to be the leader amongst ACSC member participants.