the cyberwire

The CyberWire
621 East Pratt Street, suite 300
Baltimore MD 21202–3140
editor@thecyberwire.com
www.thecyberwire.com
@thecyberwire

SINET ITSEF 2013

March 19-20, 2013 Palo Alto, California

March 19

ITSEF 2013 begins this afternoon at 1:00pm Pacific Daylight Time. SINET's Robert Rodriguez convened the gathering with a call to "innovate, inspire, and engage." The conference will work to strengthen the connections among cyber security stakeholders in a way that serves innovation. Here are some of the discussions we expect to profit from.

Steve Bowsher, Managing Partner and Executive Vice President of the CIA-funded venture capital fund In-Q-Tel, offers insights from Intelligence Community's angel investor. (Tomorrow, we'll hear from other venture capitalists on big tech trends in security and privacy.)

A workshop will explore information assurance compliance – with laws, regulations, and industry best practices. Panelist Bob Wandell notes that information assurance is complex and escapes easy capture by any checklist. Following a compliance checklist may demonstrate due diligence, but there's no substitute for good products integrated by qualified people to effectively address system risk.

Later in the afternoon, Stanford researchers will present some of their latest work on mobile security, search of encrypted data (without revealing search predicates), and how to design a next-generation mobile app store.

Evening sessions will continue the afternoon's treatment of law and regulation with a discussion of the SAFETY Act – a US statute enacted to give companies some protection from litigation over homeland security products. Presenter and SAFETY Act expert Brian Finch assures us that the law – often overlooked by cyber companies and their customers – covers cyber security products, policies, procedures, and services, including those developed and deployed by organizations in-house. DARPA will describe how performers can help it solve its cyber challenges, and NIST will cover the mission of its National Cybersecurity Center of Excellence.

The first day ended with advice from the Communications Security Establishment Canada on how to sell cyber and supply chain security solutions to the government of Canada.

March 20

In-Q-Tel's Steve Bowsher spoke yesterday and described how his organization bridges the classified intelligence world and the unclassified domain of Silicon Valley innovation. In-Q-Tel wants to make deals in advanced analytics, cloud and next-generation infrastructure, digital identity, mission tools (gaming, simulation, geolocation, etc.), and mobility (including device management, security, and ad-hoc networks).

We'd also like to pass on one insight from DARPA's presentation yesterday: to have a reasonable prospect of working with them on cyber research, performers should talk with the responsible DARPA program manager for context and insight. Proposals submitted over the transom have a reduced chance of success.

Vice Admiral Beaman's keynote today covered cyber security from the perspective of a senior operational commander. Since Sino-American tensions in cyberspace are much in the news,

we asked for his perspective on relations between the two countries. He explained that all is not conflict. "Our national policy seeks to establish a positive, cooperative, and comprehensive relationship with China, capable of addressing global challenges and advancing our shared interests, and that includes cyber security. China's military advances have enabled it to contribute cooperatively to the international community's efforts in responding to common challenges and transnational threats."

He also said, commenting on military cyber policy generally, "The Department of Defense and the Navy have taken positive, proactive steps to anticipate, mitigate, and deter cyber threats, and our success in cyberspace depends on a robust public/private partnership." Finally, he recommended reading both the Department of Defense's Strategy for Operating in Cyberspace and Navy Cyber Power 2020, linked below.

Alberto Yepez (Managing Director, Trident Capital) moderated this morning's session on moving from government business to the broader market. He thinks federal business can be a very good thing for a young, entrepreneurial cyber security company. The government's challenging security requirements and aptitude for selecting right partners to design solutions to immediate problems can be a genuine aid to building a business.

"Where the model breaks down," Yepez said, "is when these requirements force startups to create 'one-off-solutions' – custom solutions that are only applicable to specialized scenarios." He advised focusing on building a commercial solution from the beginning, avoiding the custom-solution trap through strong product management, expanding solid federal use cases to broader markets, and creating the partner ecosystems necessary to delivering customized solutions.

Terry Kramer's presentation this afternoon covered the future of the Internet, and in particular who should own it. Ambassador Kramer led the US delegation to last year's World Conference on International Telecommunications. The US didn't sign the final treaty (largely because of ambiguities that, absent clarification, could have opened the way for content censorship), but Kramer thinks that the conference's outcome nonetheless was broadly positive. Differences over whether open markets trump dirigisme as an approach to innovation aside, there's general agreement among nations that we should work toward universal broadband and effective cyber security.

There are particularly compelling opportunities for collaboration with African and Latin American nations. The US wants an environment where the Internet and telecommunications thrive, and we shouldn't let control issues trip us up. And, Kramer says, innovation is global. We need to think very broadly and pay due attention to the developing world.

March 21

ITSEF 2013 wrapped up yesterday with interesting sessions on the state and future of IT security.

The venture capital panel seemed to agree that the security sector hasn't been overvalued; new threats and new platforms give it plenty of room to run. Security is remarkable in that, unlike other sectors, it hasn't become commoditized – customers are willing to buy best-of-breed security products, services, and solutions. We also haven't seen massive security consolidation, probably because owning all the technology and integrating it is tough and those who've tried it tended to become "old, boring, and slow" (their words, not ours).

Many venture capitalists used to discourage portfolio companies from selling to governments for familiar reasons (too slow, too bureaucratic, better to start with pharma or finance, etc.) but this has begun to change, thanks in part to organizations like SINET and In-Q-Tel. Government agencies, particularly in the Intelligence Community, are now perceived as valuable early adopters, catalysts, and proving grounds.

What new technologies would attract VC eyes? A "bot wall" to block automated attacks, better endpoint security (perhaps through enhanced virtualization), mobile data management (not just mobile device management), and – very tough engineering challenges – cloud and SCADA security.

One basic tip on selling to government agencies: focus on the mission and sales will take care of themselves. In the US, the Director of National Intelligence is looking for innovative ways to procure security services as opposed to security products.

Tuesday's presentations by Stanford researchers offered insights into the future of mobile technology and app stores.

Mobile security today resembles the early days of PC security in its need to understand operating systems and applications and to apply low-level controls. But it's different in that it deals with compact, complex software tied to an integral array of sensors and interfaces (cameras, audio input/output, magnetometers, accelerometers, etc.) that yield very rich data streams. Researchers are learning how to fingerprint devices based on geolocation or even physical orientation.

The more computing power and interfaces devices gain, the more fingerprinting can enable beneficial services, productivity, and a richer user experience. (And fill in the increased opportunity for attack that this inevitably enables.)

On app stores, these were intended to be clean, safe marketplaces of verified applications. So what happened? Part of what happened is the emergence of dubious "grey-ware" – apps that some find acceptable but others reject (on privacy or other grounds). The sheer volume of apps submitted, and the market demand for quick availability, makes it difficult for any store to vet the apps it receives.

Industry has made some progress (witness Google's Bouncer), but some fundamental work remains. What, for example, makes an app "malicious" or "unacceptable"? Stanford researchers are working on data flow analysis to provide an objective measure of what apps actually do. Mapping "sources" of data on devices and "sinks" where an app sends data to can flag malicious or abusive use of APIs. Users should welcome information about what their apps actually do, and developers should welcome more uniform review.

For more follow-ups to ITSEF 2013, and for news on related topics, we invite you to keep an eye on SINET. We resume our normal publication schedule tomorrow.

the cyberwire

editor@thecyberwire.com
www.thecyberwire.com
@thecyberwire
+TheCyberWire

About The CyberWire

The CyberWire is supported by CyberPoint International and its community partners. We invite the support of other organizations with a shared commitment to keeping this informative service free and available to organizations and individuals across the globe.

Revised 8.11.15