the cyberwire

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

SINET ITSEF 2014

April 8-9, 2014 Mountain View, California

April 8

SINET ITSEF 2014 gets underway this afternoon in Mountain View, California. We'll report news from the conference as it develops. We're looking forward with particular interest to hearing the contributions of Alejandro Mayorkas (Deputy Secretary, US Department of Homeland Security), Kjetil Nilsen (Director General, Norway's Nasjonal Sikkerhetsmyndighet), and Philip Quade (Chief Operating Officer, Information Assurance Directorate, National Security Agency).

The conference's participants plan to take up issues such as identity management, automation for cyber security, the Internet-of-Things (and the "hyperconnectivity" the IoT implies), and the challenges that enterprises face—whether security, regulatory, or legal—managing mobile devices in the cloud.

Tomorrow's sessions will be of particular interest to entrepreneurs. We invite any of our readers who jump into the "Cybersecurity Shark Tank"—the name of one of the table sessions—to let us know how they fared delivering their two-minute elevator pitch to experienced industry and venture capital hands.

April 9

Yesterday's sessions encompassed several interesting topics.

During the "Guidance for Startups: Evaluating and Working with Enterprise Prospects" workshop, cyber entrepreneurs received the following advice: to sell into a large enterprise, start with a sponsor champion and have a simple value proposition that differentiates you from the field. Address a well-defined and readily understood pain-point, and don't try to do too much. Build relationships at various levels within the prospective customer's organization. Include the CFOs – they control the money. The real (as opposed to apparent) key decision-makers are usually not a company's CISO or CIO. The best strategy is to secure an early adopter willing to offer references, and then make sure you deliver what you promise.

The workshop on "hyperconnectivity" featured a very informative panel discussion. Panelists unanimously agreed that current privacy regulations don't adequately address the growing connectivity arriving with today's Internet-of-Things. Many privacy issues surround internet appliances getting, holding, and exposing personal information (consider, for example, information derived from map and mobile device programs). People enter personal information into devices and applications without realizing that they're exposing that information to, effectively, the world. Users tend to be either naïve or uncaring until some incident causes them to suffer from that exposure. (Then they become aware and start to care.) Panelists suggested that we need more innovation in awareness-based security as opposed to the current barrier-based approach. We should begin with the assumption that data will be shared, and then work to protect those data's contents and foster awareness of what's being shared. And, as elsewhere, automation would help: we need automated tools to handle data protection.

In the "CyberSecurity Automation" workshop, panelists Peter Fonash (Chief Technology Officer, Cybersecurity and Communications, US Department of Homeland Security) and Phillip Quade (Chief Operating Officer, Information Assurance Directorate, US National Security Agency) described toolsets for Active Cyber Defense and a plug-and-play tools framework for interoperability and automation. The Department of Homeland Security particularly emphasized the importance of automated information sharing; cyber defense generally needs quick, rapid command and control once an intrusion is detected. The panel emphasized that the solution is not more trained cyber experts, but rather better use of automated techniques to keep pace with rapidly advancing cyber threats. The US Federal Government plans to solicit industry input to put towards new reference architecture for Active Cyber Defense.

SINET ITSEF 2014 continues today, and we'll publish a final wrap-up issue on the conference tomorrow.

April 10

SINET ITSEF 2014 wrapped up yesterday, and this is our final special issue devoted to the conference. We will, however, publish exclusive interviews with some of the participants over the next two weeks.

A panel on big data (with ManTech, In-Q-Tel, ZL Technologies, and the US Department of Homeland Security participating) addressed the pervasive siloing of big data without adequate means of using data across silos. Big data's privacy challenges were also addressed: since a new framework is needed for sharing data, any such framework should have privacy protection built in. Privacy won't be secured if it's treated like an add-on or an afterthought.

Mark McLaughlin, President and CEO of Palo Alto Networks, asked the conference to think about what counts as winning in the current age of advanced cyber threats. He argued that the traditional approach of detection followed by remediation no longer works given the exponential growth of adverse cyber events. The continuing shift to the cloud and virtualization has tipped, and continues to tip, the scale in favor of bad actors: they now have a larger attack surface with more access points to the systems that they target. Our goal in devising next-generation security should be what he called "Prevention Intelligence." Examples of this would be embedding prevention techniques into new operating systems and sharing threat intelligence across platforms.

Alejandro Mayorkas, Deputy Secretary of the US Department of Homeland Security, delivered the first of two keynote addresses. He focused on his department's major initiatives to engage entrepreneurs in development of next-generation cyber technology. (The CyberWire will be publishing an interview with Deputy Secretary Mayorkas within the next two weeks.)

Entrepreneurs are keenly interested in their exit strategies, and executives from ArcSight, Cloudera, SourceFire, Morta, Blue Coat, and Solera Networks shared their lessons learned. A common theme was the importance of leveraging early adopters for their products, thus getting early market validation that they can subsequently scale as they grow their business. There was consensus on the importance of keeping one's early focus on a set of guiding principles, and then being alert to changes in markets and environments (and nimble in responding to them).

Stanford University's Vivek Wadhwa offered a predictive look at how advancing technologies were likely to prove disruptive. He sees manufacturing by cheap labor in China and India being disrupted by robotics. Robots able to produce goods more cheaply than human labor will return manufacturing to countries like the United States. Eventually, as technologies like 3-D printing are commoditized, even robotic manufacturing in centralized plants will tend to be replaced by self-manufacturing in the household.

Allegis Capital's Robert Ackerman moderated a panel composed of investors from Highland Capital Partners, Kleiner Perkins Caufield Byers, and SineWave Venture Partners. Continued

strong growth across the security sector through the next five years warrants continued venture investment in cyber startups. The government remains a large and important market: it accounts for one third of cyber spending today. The IPO and M&A markets in the cyber sector are growing and remain strong in comparison with other IT and technology areas. The panel thought Bromium, MobileIron and vARMOUR were three good examples of promising young companies.

Kjetil Nilsen, Director General, Nasjonal Sikkerhetsmyndighet (NSM - Norway's National Security Authority) delivered the final keynote. The NSM is responsible for all aspects of cyber security in Norway, and Director General Nilsen gave the conference a useful perspective from an agile and advanced country that punches far above its weight in cyber security. The CyberWire will publish an interview with Director General Nilsen 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 8.4.15