

INTERVIEW: SINET sees public/private partnerships as future for cyber security space

9 Jan 2012

The Security Innovation Network (“SINET”) is a US-based organization that promotes the advancement of innovation and collaboration in the cyber security domain, and connects buyers, researchers, investors and builders in that space. It operates across several platforms, providing advisory/consulting services, organizing programs across the US to promote innovation and research, as well as managing a membership program.

The Department of Homeland Security’s (“DHS”) Science and Technology Directorate has supported SINET for the past seven years. Sponsors also include Google, Trident Capital, SalesForce.com and the US Department of Defense, among others.

Some recent examples of work include putting US scientific and technology applications firm SAIC, Inc. (NYSE: SAI) in contact with Stanford University, Facebook and the DHS to collaborate on an app security hackathon.

Speaking to Global Security pipeline recently, Robert Rodriguez, Chairman and Managing Principal of SINET, pointed out that the US Defense Industrial Base – contracting corporations such as Boeing, Lockheed Martin, General Dynamics and small and medium-sized contractors, as well as the civilian government and the defense department - are missing approximately 50 to 70% of all early-stage emerging technology companies in the market.

“How does the entrepreneur, the one who is bringing the innovation to market, get recognized and get his voice heard to access the ecosystem of venture capital, risk capital, IP protection, legal advice, regulatory principles opportunities in the market – these things are not interchangeable for our entrepreneur,” Rodriguez said. “Importantly, who is going to connect him to the government, the closed, very connected, well-informed community of Washington, D.C. - the National Security Agency, the Defense Information Systems Agency or the DHS. That’s where we intervene to help connect the small business community and promote the development of public/private partnerships.”

In addition, he said the scale of the cyber security issue has only been brought to attention recently, especially in the industrial sector: “Where the public sector focuses on mission-readiness and no margin for error, the industry is very much about shareholder value and, as a consequence, where budgets should be allocated. CISOs have had a tough time bringing the issue of IP protection and technology to light.”

This news service has reported that technology will indeed be a key differentiating factor in the defense and security sector, and, as such, organizations will need to be able to access it to get ahead in the market. “When it comes to innovation, you cannot afford to leave any stone unturned – you need to be aware of what technology is available for mission-critical or infrastructure needs etc,” he said. “Government budgets for cyber security are up across the board – that in itself says ‘cyber security is an issue we need to address’. In addition, the appointment of a US Cyber Security Coordinator [Howard Schmidt] a couple of years ago, and several other key figures in the DHS, DoD, DoS show that the issue is being taken very seriously.”

According to him, some of the areas that are set to grow in importance are “Big Data” analytics, software assurance and the issues arising from the general interconnection of millions of networks, including social networks. Importantly, he believes privacy could overtake security as one of the main concern for consumers and be the source of further complications in the cyber space.

Please contact Robert Rodriguez, Chairman and Managing Principal at SINET, at rdrodriguez@security-innovation.org for more information on SINET

Please contact the reporter on this story, Amélie Labbé Thompson at amelie.labbethompson@vbresearch.com