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

SINET Baltimore Policy Summit

April 15-16, 2013 Baltimore, MD

April 16

After a greeting from CyberMaryland's Rick Geritz, SINET's Robert Rodriguez introduced the evening's panelists: Jason Kaufman (Managing Director, the Chertoff Group, who served as moderator), Scott Aaronson (Director, Government Affairs, Edison Electric Institute), Leonard E. Moodispaw (CEO, President, and Chairman, KeyW), Tyler Winkler (Executive Director, Dell Secure Works), Jerry Archer (CSO, Sallie Mae), and Sherri Ramsay (Director of Threat Operations, CyberPoint International, and former Director of the National Threat Operations Center).

Sherri Ramsay characterized the evolution of the cyber threat as revealed by its characteristic tools. These were originally designed for espionage, expanded to disruption, and have now evolved into destructive instruments. The original target was the US Department of Defense, but the target set has expanded to civilian agencies and businesses of all sizes. She identified effective and actionable information sharing as the common challenge that the government and industry confront.

Disclosure of incidents, vulnerabilities, and threat information is obviously invaluable, but Leonard Moodispaw argued that, outside of the energy and financial sectors, disclosure isn't yet what it ought to be. Securities and Exchange Commission rules haven't so far made disclosure as widespread as it should be (and too much disclosure is buried in corporate annual reports somewhere behind "janitorial services"). Ramsay thought more effective anonymity would have a particularly healthy effect on information sharing. Archer suggested experience sharing as opposed to mere data sharing.

Tyler Winkler said it's common for a start-up to lack an effective go-to-market focus: they tend to chase revenue opportunities indiscriminately. The beginning of wisdom in his own company's history was the recognition that legislation had shaped the managed security market by setting up an initial market for compliance work. Jerry Archer noted (with other panelists concurring) that the first lesson of compliance is automation: "You unburden yourself from compliance though automation," and this is of direct economic benefit. Automating compliance saves money and enables more efficient allocation of human, technical, and financial resources.

The electrical power sector is, claimed Scott Aaronson, the only sector under mandatory cyber security guidelines. Compliance amounts to a 90% security solution, with the next 9.99% coming through close and continuous coordination among government and commercial actors. This leaves an irreducible amount of risk that can be managed but never entirely eliminated—we cannot throw money away in the vain pursuit of perfect security.

Speaking as a consumer of security solutions, Archer advised cyber entrepreneurs to look for opportunities in niche innovations that yield an immediate return. He'd like in particular to see tools that can go into a production environment without disrupting it.

Winkler said managed security can be an excellent solution for smaller companies, and Archer foresaw cloud providers moving security to a new level over the next three to five years.

Moodispaw advised businesses not to neglect user training, and Ramsay summed up with a call for better "network hygiene": patching known vulnerabilities, sound password management, thoughtful privilege management, etc. She strongly advocated re-conceptualizing system administrators as system defenders.

After the panel discussion, Maryland's Governor Martin O'Malley discussed cyber policy as an engine of job-creation. He views Maryland, he said, as unusually well suited in terms of workforce and customer base to serve as a platform for cyber innovation and "the nation's cyber security infrastructure." He called for continued work on better standards for cyber security.

The day's final speaker was (retired) General Michael Hayden, formerly US Director of Central Intelligence and Director of the National Security Agency and currently a principal with the Chertoff Group. He made four points: First, we should expect the cyber threat to get worse. There are many bad actors ("sinners") in the cyber domain: nation states, criminals, and hacktivists. States, the most capable cyber threat, are also, at some level, accountable for their actions, and can be deterred. Criminals are essentially parasitic, and like most parasites, don't wish to destroy their host. Hacktivists, currently the least capable, are in many respects the most frightening. Motivated by extravagant aspirations (if not by frank nihilism) they are unsatisfiable and undeterrable. And the trend in all three groups is toward greater capability.

Second, "the cavalry isn't coming." In the United States, Cyber Command hasn't been given either the legal or policy authority to act freely in the cyber domain. No national consensus means no comprehensive national response.

This means, third, that the private sector will ultimately provide security for the network as a whole. He drew an analogy from the American Civil War, where the "supported command" maneuvered, and the "supporting command conformed its movements to the supported command." The government is the supporting command, the private sector the supported command. How can public policy recognize this relationship? Hayden brainstormed some instructive analogies. What about a cyber stand-your-ground law? Could we organize cyber posses as need arose? We might not go so far as to issue letters of marque and reprisal, but some such measures might well be considered.

Fourth, he asked the conferees to consider the traditional risk equation: Risk = (Threat) (Vulnerability) (Consequence). Most of our energy has been devoted to reducing vulnerability. This, he suggested, mainly keeps the incompetent out, and it's important to do that. But the center of gravity has shifted to consequence. The "presumption of breach" should lead us toward self-awareness about our networks and the threats they face.

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