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

Billington Cyber Summit

September 16-17, 2014 Washington, DC

September 16

Admiral Michael Rogers, NSA Director and Commander, US Cyber Command, delivered the conference's opening keynote. He asked, how can we achieve security in cyberspace when the level of activity against us continues to increase so dramatically?

No single technology, no single actor, offers a comprehensive solution for cyber security, and yet organizations have focused on stopping penetration of networks. This is misguided. Resiliency should be our goal: we should work toward being able to accomplish our mission in the face of damage and degradation. Despite our best efforts, we'll sustain damage. There's an obvious analogy to shipboard damage control — you control and fix damage as you continue to operate. So, we should focus on operating and mediating simultaneously.

This led to the admiral's discussion of five challenges we face in cyber security.

Having to fight through damage and degradation is a major change in mindset, and this is our first challenge. Getting the right mindset requires leadership buy-in. It requires thoughtful reconsideration of resources and roles.

The next challenge is achieving situational awareness. How to do so requires the sensing and visualization of networks. You can't simply bolt on defensive capability; redundancy, resiliency, and defensibility must be built into our systems.

The third challenge is getting the right partnerships — cyber security isn't a pick-up game, but we've tended to treat it as such. And here, Admiral Rogers asked for the private sector's help in building long-term partnerships.

The fourth challenge is authorities, and getting the right authorities to ensure resiliency. Information assurance is part of our mission. We need to work through the partnerships that will share information, the pathways for doing so, and the kind of information we'll share.

The fifth and final challenge is building the workforce that can provide resiliency. Building that workforce also depends on partnerships and relationships.

The bottom line is recognition of the problem and developing the partnerships to deal with it. Admiral Rogers concluded by noting how pervasive cyberspace has become to life as it's lived today. What happens when we lose confidence in our systems? When we no longer believe our data? We need to recognize this challenge, and partner to meet it.

The conference is continuing with additional speakers and panels. The CyberWire will report on these in tomorrow's issue.

September 17

The consensus on cyber resiliency? Chasing perfect cyber defense is a mug's game. While traditional perimeter defenses, especially defenses-in-depth, have their place, the future lies in detection, mitigation, management, and mission assurance.

Current NSA Director Rogers and former NSA Director Hayden offered different metaphors for this approach to resiliency. Rogers likened it to shipboard damage control. You expect warships to sustain damage in combat, and you prepare for it. You identify, contain, and repair damage as soon as you can, and you do it in a way designed to maintain or restore mission capability. Hayden chose a biological metaphor: consider the way an organism responds to injury or infection and the way it restores itself, because here, again, injury and infection are expected.

Cyber attacks are to be expected because of the large number of actors and the sheer complexity of cyberspace. FireEye's Dewalt warned of the tremendous current interest in offensive activities — some 500 organizations in 204 countries are involved in offensive cyber operations. Nearly all critical-infrastructure companies are being breached weekly, and adversaries are becoming more effective. Former NSA Director Hayden sees those adversaries as falling into three tiers: states, gangs, and the disaffected (listed in decreasing order of capability). States tend to be self-limited, gangs are hired guns, but the disaffected, although currently the least capable, are in some ways the most worrisome. Their motives are obscure, and they are less susceptible to deterrence or negotiation. And the disaffected are beginning to acquire capabilities we associate now with low-end nation states.

Attackers find ample opportunity to work in the vulnerabilities that the sheer complexity of cyberspace inevitably presents. The closing keynote speaker, NIST's Ronald Ross, described three tiers of vulnerabilities: known vulnerabilities (the kind fixed on Patch Tuesday), unknown vulnerabilities (zero-days), and adversary-created vulnerabilities (such as advanced persistent threats).

Partnership — across all levels of government, the private sector, and internationally — was agreed to be essential. But barriers to effective collaborative defense remain. White House Cybersecurity Coordinator Daniel noted the inherent difficulty of the problem: the psychology and economics of cyberspace, he thinks, remain imperfectly understood, and this is particularly true of the incentives that operate in that domain. Efforts like the NIST framework (also commended by DHS Deputy Undersecretary for Cybersecurity for NPPD Schneck) are a solid start, but remain works in progress. Schneck noted the difficulties involved in sharing information that's often classified (and over-classified).

Many of the speakers mulled the tension between privacy and security, and counseled a need for balance. Improved transparency (or perhaps, as Hayden suggested, "translucence") on the part of government would help matters here. Former NSA executive Chris Inglis in particular thought this was an important policy lesson from the Snowden affair. Espionage has traditionally been an executive function, Hayden observed, and Congressional and judicial oversight, as in the US, are international outliers that afford an opportunity for improving transparency. "NSA surveillance blew up," he said, "because of a significant change in US political culture. People stopped believing that consent of the governors was equivalent to consent of the governed."

Cyber security needs to move away from its preoccupation with network security to become data-centric. Inglis and Venture capitalist Ted Schlein in particular called this out. Inglis emphasized that the value lies in the data, and that assessing that value, and protecting it, is a corporate board level issue. "Bad guys don't care about the network," Schlein noted, "They care about data." Frictionless key management would represent a tremendous advance in data protection. Anti-virus will evolve into breach detection and management, and this, he believes, will amount to a new industry. He also sees signature-based endpoint security as on its way out. Security analytics, threat feeds, and next-generation endpoint security are trending among VCs.

In sum, cyber resiliency requires credible and rigorous risk analysis and vulnerability management. It needs to be pursued collaboratively, and within the context of realistic goals and well-founded best practices.

See the daily issue for other accounts of the Summit and background on the issue of cyber resiliency.

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