the cyberwire

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

President's Cyber Security Summit

February 13, 2015 Palo Alto, California

THE CYBERWIRE (Monday, February 16, 2015) — We had planned to take today off for the Presidents' Day holiday, but the current US President's Friday cyber security summit in Silicon Valley has changed our minds. We therefore offer this brief account of that summit, the executive order signed there, and reactions to both.

President Obama met at Stanford University with industry leaders to outline his plans to enhance cyber security, to push for more industry cooperation with the government, and to make a plea for more effective cyber-threat information sharing. The meeting did succeed in bringing serious, senior business leaders together (despite the animadversions represented by the much-noted absence of the Google, Facebook, and Yahoo CEOs). The industry leaders present generally supported the NIST Framework, encouraged mutual threat information sharing, and asked for liability protections (especially with respect to information shared with the government). Industry support for the NIST Framework seemed particularly pronounced.

The President was particularly concerned with threat information sharing, casting it as important to both economic and national security (making the right sorts of soothing noises about security needing to respect civil society, privacy, and civil liberties).

The centerpiece of his appearance was signing an executive order, "Promoting Private Sector Cybersecurity Information Sharing." The order's key elements are:

- Creation of "information hubs," more formally "Information Sharing and Analysis Organizations" or "ISAOs." He envisions these as loci where stakeholders can share information on particular threats in specific economic sectors or geographical regions. The ISAOs would be private and voluntary bodies (and the executive order specifies that they can be organized by either for-profit or not-for-profit organizations) that would also establish voluntary standards for their members.
- A directive that the Secretary of Homeland Security will "strongly encourage" the formation of ISAOs. The Secretary will also ensure that his department's National Cybersecurity and Communications Integration Center (NCCIC) will "engage in continuous, collaborative, and inclusive coordination" with the ISAOs.
- Authority for the NCCIC and the new national Cyber Threat Intelligence Integration Center (CTIIC) to share threat data with the ISAOs. Some of the data are envisioned to originate from classified sources, and the decision whether to release such data through the Department of Homeland Security will reside with the Director of National Intelligence (presumably acting through his CTIIC).
- A call to the ISAOs to develop and abide by appropriate privacy protections.

This Executive Order is advisory with respect to the private sector (to be expected, since a president cannot direct the private sector to take action except in extreme circumstances, and President Obama isn't prepared to claim the nation's in extremis with respect to cyber security). The CTIIC's role remains, so far, unformed — there was a sense among those in attendance that the new center is still in its aspirational stages.

Access to classified intelligence is an interesting piece of the information-sharing plan, but since authority to release such information to the Department of Homeland Security for further sharing rests with the Director of National Intelligence, it's unclear how much will actually change.

The executive order's provisions to permit both for-profit and not-for-profit entities to form ISAOs recognizes the various industry information-sharing efforts currently in progress, probably evincing a desire not to unravel work that's already been done.

How the executive order works out in practice remains to be seen. The devil, as one knowledgeable observer told us, is here elsewhere in the details.

Some areas of interest that received relatively little attention at the summit included breach notification practices (or regulations), STEM education, and Computer Fraud and Abuse Act reform.

Apple's CEO Tim Cook was among the most prominent industry leaders to participate. He took the opportunity to underscore the importance of industry's commitment to customers' privacy. This, of course, highlights Apple's differences with some elements of the government (notably within the Justice Department) over encryption, and also with some of Apple's competitors. ("If you're not paying for the product, you are the product," may be what Fortune calls a "cyber chestnut," but it does signal what Apple thinks sets it apart from Google, Facebook, and Yahoo.)

Industry both anticipated and responded to the White House initiatives with a flurry of threat intelligence and information-sharing solutions and consortia. FireEye jumped into this market space (as Facebook did early last week), and the Cyber Threat Alliance announced four new industry members. Reactions come from the UK's cyber security sector, as well: Computer Business Review had a rundown. Back stateside, the US Attorney for the Western District of Pennsylvania thinks that anyone interested in seeing cyber information sharing done right should look toward Pittsburgh. (That's not pure hometown-ism, either — a number of high-profile investigations of Chinese industrial espionage have been developed in the Steel City.)

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