Akin®

White House Holds Cybersecurity Summit at Stanford University

Feb 18, 2015

Reading Time : **4 min**

By: Francine E. Friedman, Natasha G. Kohne, Matthew Thomas (Senior Public Policy Specialist) David S. Turetsky, Visiting Professor, College of Emergency Preparedness, Homeland Security, and Cybersecurity at the University of Albany

The EO encourages private organizations to develop information sharing and analysis organizations (ISAOs), which may be nonprofits, membership organizations or a private company. It also directs the Department of Homeland Security (DHS) to fund a non-profit organization to develop a common set of voluntary standards for ISAOs, and clarifies the agency's authority to enter into agreements with ISAOs. Further, the EO adds DHS to the list of Federal agencies that may approve classified information sharing arrangements and takes steps to ensure that information sharing entities can appropriately access classified cybersecurity threat information.

While broadening the ability of the federal government to share threat information, the EO also emphasizes personal privacy. Under the EO, private sector ISAOs must agree to abide by a common set of voluntary privacy standards, which must include privacy protections, such as data minimization, for ISAO operation and ISAO member participation. Additionally, agencies collaborating with ISAOs under the EO will be required to coordinate their activities with their senior officials for privacy and civil liberties and ensure that appropriate protections for privacy and civil liberties are in place and are based upon the United States Federal Trade Commission's Fair Information Practice Principles.

The President's Remarks

In addition to stressing the importance of information sharing and signing the EO, the president highlighted several companies working to support the administration's

cybersecurity initiatives. "I want to acknowledge, by the way, that the companies who are represented here are stepping up as well. . . . You've got companies from Apple to Intel, from Bank of America to PG&E, who are going to use the Cybersecurity Framework to strengthen their own defenses. As part of our BuySecure Initiative, Visa and MasterCard and American Express and others are going to make their transactions more secure. Nationstar is joining companies that are giving their companies [customers] another weapon to battle identity theft, and that's free access to their credit scores." The president also announced a "Cyber Threat Alliance," that includes companies like Palo Alto Networks and Symantec, which will work to implement the threat sharing protocols that are stipulated under the EO.

The president, several high-ranking administration officials, and a number of participating business leaders also called on Congress to pass information sharing legislation that could provide business with liability protections for the sharing of appropriate threat information. The president emphasized that this is not a partisan issue. The president and certain administration members also called on Congress to fund the Department of Homeland Security, with funding currently scheduled to run out late this month.

The president emphasized evolving cybersecurity and privacy issues as a major challenge of this century, implicating national security, economic security and prosperity, and family security. The technologies that "empower us" he said can "undermine us." He discussed threats, needs, opportunities and actions in these areas, and said further privacy proposals from the administration would be coming later this month.

Our partner, David Turetsky, was invited by the White House to attend the summit, and also attended meetings at Stanford organized by the National Institute for Standards and Technology (NIST) the day before. His observations from the summit and those meetings include:

- Unauthorized Access Will Occur: Companies repeatedly said that there are only two kinds of companies, those who know they have been hacked and those who do not know it. Speakers emphasized that monitoring and earlier detection are important as are other efforts to make entry, exfiltration and destruction more expensive and less valuable for intruders (*e.g.*, through two-factor authentication rather than passwords, up-to-date encryption, certain storage techniques, etc.), but the expectation is that entry will occur.
- Cyberattacks Can Affect All Sectors: Some speakers noted that after the Target data breach, many other companies distinguished that experience by noting they are not in

the retail space. The Sony experience has changed that perspective for many.

- Cybersecurity is a Key Component of Risk Management Strategy: Some companies find that the threat landscape changes so rapidly, in turn affecting their cybersecurity risk profile, that they reassess and budget for security monthly rather than annually; some also said that they think of these issues as fundamental to "trust" and directly related to their investment in their brand, which enters into their assessment of the stakes in this area.
- Private Sector Facing Increasingly Sophisticated Attacks: Experts noted that there used to be a lot of talk about military-grade cybersecurity protection but that grade of protection is increasingly moving into the commercial sector, an occurrence that reflects that sometimes the same or even more sophisticated attacks are made on the commercial sector.
- Compliance Burdens May Hinder Security and Mitigation Efforts: In certain industries that are also subject to state regulation, a couple of speakers noted with concern that they are increasingly spending time and effort on "compliance" rather than improving cybersecurity; others noted that there are some laws that are impediments to consumer protection, with one stating that one such law can prevent a company from texting all of its customers after a security breach, preventing a method to make timely and effective notification that can limit the window for fraud.
- Cybersecurity by Design: Speakers noted that opt-in security is usually not effective and that often users do not cooperate. There has to be an effort to design security in. Some observed that perhaps the highest level of security requirements should attach to senior IT and other executives who have the most access, since their credentials may be the most valuable to hackers.
- Greater IT/Security Training: Some participants suggested more training needs to happen at many levels. For instance, some claimed that that possibly 25 types of programming errors account for the lion's share of software vulnerabilities and that this can be improved substantially through training and much better feedback.
- Cyber Attacks Can Have Physical Consequences: The problems encountered down the road could be far worse in terms of impact than those encountered so far. Some examples given by speakers who said they were looking ahead include possible manipulation of industrial control systems worse than that which recently damaged a German steel plant, and the changing of sensitive records, such as medical records, that could result in serious harm, including death.

Categories

Cybersecurity, Privacy & Data Protection