Portfolio Media. Inc. | 860 Broadway, 6th Floor | New York, NY 10003 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

Presidential Summit Reveals Cybersecurity Concerns, Trends

Law360, New York (February 17, 2015, 5:41 PM ET) --

Angelique Kaounis

On Feb. 13, 2015, President Obama held a White House Summit on Cybersecurity and Consumer Protection at Stanford University. The event was attended by members of Congress, industry and tech company leaders, law enforcement, students, and others, with the goal of "work[ing] together and explor[ing] partnerships that will help develop the best ways to bolster our [nation's] cybersecurity."[1]

The summit took a broad approach to addressing cybersecurity issues — from discussing the intersection between foreign nations and U.S. law enforcement, to presenting cybersecurity as a business differentiator. Speakers and panelists included the president himself; CEOs from top technology, utility, health care, cybersecurity, insurance, banking and credit card companies; representatives from interested nonprofits; and officials from the U.S. Department of Energy, the National Security Council, the FBI and the White HouseOffice of Science and Technology Policy, among others.

The summit comes on the heels of the president's recent proposal to increase certain penalties for violating the federal Computer Fraud and Abuse Act, his call on Congress to pass legislation that promotes greater information sharing between the government and the private sector, and the administration's announcement of the creation of the Cyber Threat Intelligence Integration Center to coordinate real-time analyses of cyberthreats between governmental agencies and the private sector.

Assessments of the Current Cybersecurity Landscape

If there was one message that came through loud and clear at the summit, it was that cybersecurity is not just a consumer data issue, or a national security issue, or an industry competition issue — it is a worldwide concern that affects everyone who uses the Internet or taps into the electrical grid. This theme permeated the observations and guidance provided by a multitude of panelists from across the spectrum. Other key points included the following:

1. This is not a static environment.

Across the board, speakers commented that the cybersecurity landscape is ever-changing. Cyberattacks

"are getting more and more sophisticated every day."[2] For this reason, President Obama made clear that "we've got to be just as fast and flexible and nimble [as the criminals and hackers] in constantly evolving our defenses."[3]

2. What's good for our customers is good for us.

Jeff Zients, director of the National Economic Council and assistant to the president for economic policy, observed that cybersecurity and consumer protection are two sides of the same coin.[4] Economic loss attributable to a lack of cybersecurity includes not just the theft of intellectual property and increased cost of doing business due to data breaches, but also the hidden cost of delay in adopting new technologies. In turn, this delay affects the competitiveness of U.S. companies and the products and services available to consumers. Hacking also negatively affects companies' brand value and undermines consumer confidence. At every level, cybersecurity is essential for the health of the economy.

In the area of electronic payment processing, several industry leaders made it clear that they have been, and will continue to implement a broad range of measures to ensure "that electronic payments, financial settlements, and the IT systems and data that support this financial activity, are reliable, trusted, and secure."[5] These include tokenization, "chip and pin" or "smart" credit cards, and biometric authentication, as well as an increased focus on fraud detection through risk and data analytics.

3. We're all in this together.

As noted above, President Obama recently introduced several measures aimed at promoting the sharing of information between government agencies and private industry players, and coordinating cybersecurity assessment across these layers. At the summit, the president emphasized that cybersecurity must be a joint mission between the private sector and government, sharing appropriate information as partners.[6] In furtherance of this goal, the president signed a new executive order at the summit to promote more information sharing about cyberthreats, both within the private sector and between government and the private sector.[7] The order will encourage more companies and industries to set up organizations — known as "hubs" — so they can share information with each other.[8] It will call for a common set of standards, including protections for privacy and civil liberties, so that government can share threat information with these hubs more easily.[9] And, according to the president, the order can help make it easier for companies to get the classified cybersecurity threat information that they need to protect themselves.[10]

Of course, this type of large-scale information sharing is not without concerns, and both industry leaders and consumer advocacy groups emphasized the need to protect consumer privacy when engaging in such conduct. President Obama echoed this concern, explaining that the government has to make sure it is "protecting the privacy and civil libert[ies] of the American people" by safeguarding personal information when sharing information about cybersecurity threats.[11] And "[w]hen consumers share their personal information with companies, they deserve to know that it's going to be protected."[12]

To this end, the White House will be proposing legislation called the Consumer Privacy Bill of Rights to give Americans baseline protections, such as the right to decide what personal data companies may collect from individuals, and the right to know how companies are using that data. The White House will also propose the Student Digital Privacy Act, which is aimed at addressing the collection of data for marketing purposes.

Industry participants also called for information-sharing to be a two-way street, with the government giving as much as it gets. One panelist observed that "information sharing may be the single, highest impact, lowest cost, and fastest way to implement capabilities we have at hand, as a nation, to accelerate our overall defense from the many varied and increasing threats we are facing every second."[13]

4. Make someone accountable — or better yet, make everyone accountable.

Secretary Penny Pritzker of the U.S. Department of Commerce quoted a recent survey by PriceWaterhouseCoopers which revealed that only 45 percent of CEOs are "extremely concerned" about cybersecurity threats. She was amazed that this number was not 100 percent.

President Obama reiterated that cybersecurity should be everyone's concern. According to the president, to more effectively address the issue, each sector must focus on doing what it does best.[14] The government cannot secure the computer network of private businesses, and companies do not have the awareness or the ability to coordinate a response in real time.[15] Lisa Monaco, homeland security adviser to the president, similarly stressed that cybersecurity requires the use of all tools at our disposal: diplomacy, economic clout, intelligence resources, law enforcement expertise, competitive technological edge, and, if necessary, military power.

5. Prepare, prepare and prepare some more — and then consider buying insurance.

Preparation runs the spectrum — from Department of Energy laboratories testing secure grids to private companies performing "dry runs" of potential breaches (phishing emails, etc.) to test the effectiveness of their security, detection and response measures. But even the best-prepared companies are vulnerable to human error. For this reason, among others, insurance may be important. Yet, one prominent insurance industry executive noted that cybersecurity insurance is woefully underutilized.

Takeaways for Planning Cybersecurity Programs

To be adequately informed about and prepared for cybersecurity threats — and to minimize loss of IP and potential liability for data breaches — companies should carefully consider relevant practices described at the summit.

Lisa Monaco suggested that everyone should employ basic cybersecurity measures, such as following the National Institute of Standards and Technology cybersecurity framework. According to the president, leading technology and financial companies "are going to use the Cybersecurity Framework to strengthen their own defenses."[16] In light of this widespread implementation, the NIST cybersecurity framework will likely serve as a benchmark against which a company's security efforts are measured in litigation, regulatory, and other matters. In fact, one credit card company executive noted that adherence to the NIST framework may be a relevant factor in determining insurance coverage.

Separately, when it comes to voluntary information sharing and breach reporting, companies should consider that the government and law enforcement have unique tools at their disposal and may be able to act much more quickly than a private actor. As one speaker commented, the government has both attribution and admonition power — finding out who is responsible for a data breach and publicly remanding the bad actor for its conduct. To some, these are formidable reasons to contact the government early and initiate an information exchange. Another reason is response proportionality — i.e., if a large corporation is infiltrated by a foreign nation, a more effective and appropriate response

may need to come from another nation as opposed to the breached company alone.

As for accountability and preparedness, one commentator suggested asking your chief information security officer (CISO) — after you've appointed one — the following questions:

1. How would you break into our system(s)?
2. If we had a breach, would we detect it (and how)?
3. What would we do if someone did break in?

If the CISO does not have answers, s/he needs to obtain them.

Conclusion

Cyberattacks can have wide-ranging effects on our nation's economy and security. Thus, creating a comprehensive and resilient detection and defense network across industry and government is everyone's responsibility. Discounting cybersecurity concerns, for example by ignoring industry standards, may result in potential liability or a loss of competitive edge. To prevent such outcomes, companies should strongly consider cybersecurity information sharing and industrywide standards such as the NIST cybersecurity framework in implementing best practices in cybersecurity.

—By Angelique Kaounis, Gibson Dunn & Crutcher LLP

Angelique Kaounis is of counsel in GIbson Dunn's Century City, California, office

The author wishes to thank Gibson Dunn partner Alexander H. Southwell and associates Jonathan N. Soleimani, Andrew D. Tan and Zhou Zhou for their valuable contributions to this article.

[1] http://www.whitehouse.gov/blog/2015/02/13/president-obama-speaks-white-house-summit-cybersecurity-and-consumer-protection, visited Feb. 14, 2015.

[2] http://www.whitehouse.gov/the-press-office/2015/02/13/remarks-president-cybersecurity-and-consumer-protection-summit, visited Feb. 14, 2015 (hereinafter "Presidential Cybersecurity Remarks").

[3] Id.

[4] Summit speeches can be viewed at https://www.youtube.com/watch?v=KlTo9hFAFXs.

[5] http://www.whitehouse.gov/issues/foreign-policy/cybersecurity/summit#section-agenda, visited Feb. 14, 2015.

[6] Presidential Cybersecurity Remarks.

[7] Id. Currently, many industries have an Information Sharing and Analysis Center (ISAC) that helps to protect businesses, operations, and services in their respective sectors.

[8] Id.

[9] Id.

[10] Id.

[11] Id.

[12] Id.

[13] https://www.youtube.com/watch?v=KlTo9hFAFXs, last visited Feb. 17, 2015.

[14] Id.

[15] Id.

[16] Id.