WILMERHALE

Cybersecurity: Washington Week in Review, Week of February 28

MARCH 4, 2016

Tech Industry, Government Leaders Gather for Annual RSA Conference

This week, 30-40,000 attendees—including some of the biggest names in cybersecurity from industry and government—gathered in San Francisco for the annual RSA conference. Among the government attendees and speakers were Defense Secretary Ash Carter, Attorney General Loretta Lynch, National Security Agency Director Admiral Mike Rogers, the Department of Homeland Security (DHS) cybersecurity leadership, House Homeland Security Chair Mike McCaul (R-TX), and officials from the Departments of Commerce, Energy, State, and Agriculture. Among the highlights:

- Defense Secretary Carter acknowledged that the military is using cyber tactics against ISIS, including by "interrupt[ing] their ability to command and control forces, to make them doubt the reliability of their communications, to take away their ability to control the local populace." Secretary Carter also announced a new "Hack the Pentagon" bug bounty program, which will pay hackers who find vulnerabilities in public Department of Defense (DoD) web pages. Also that day, DoD announced the establishment of the Defense Innovation Advisory Board. The Board, led by Alphabet (Google) chair Eric Schmidt, will be aimed at bringing Silicon Valley's culture to DoD.
- Eric Sporre, deputy assistant director at the FBI's cyber division, said he wants companies who have been hacked "to report it to the US government agency [they] have a relationship with."
- Jamie Danker, head of the DHS National Programs and Protection Directorate's Privacy Program, discussed implementation of the new information-sharing law, and what kind of personal information will be shared, saying: "If you don't collect data in the first place, you don't have to protect it."
- Andy Ozment, assistant secretary of DHS's Office of Cybersecurity and Communications, said that the recent cyber attack on the Ukranian electrical grid should be a wake-up call to U.S. companies, who may read about the hack and be surprised.
- State Department official Christopher Painter, speaking on last year's cyber agreement with China, said that "[t]he Chinese, I'd say, never accepted a distinction that there was theft for commercial purposes or intelligence gathering."

- US Attorney David Hickton, speaking about the 2014 indictment of five Chinese PLA officials, said he “intend[s] to bring these individuals to justice. This was not just for show, or name and shame.”

US to Renegotiate Export Control Agreement

On Tuesday, March 1, the Obama administration told lawmakers that it would seek to renegotiate the 41-nation Wassenaar Arrangement’s provisions limiting the export of cybersecurity products. Specifically, the agencies will seek removal of limits on sales of “technology” needed to create “intrusion software,” which would address industry’s main concern regarding the agreement: that an overly broad definition of “technology” would restrict routine cross-border data flows about cybersecurity threats. However, there is still debate within the administration over how more limited controls on hardware and software exports necessary to develop and control intrusion software will be regulated. While industry wants these controls removed, the State Department hopes that the provision can be revised but still restrict repressive regimes’ access to spyware. Representative Jim Langevin (D-RI) praised the announcement as “a major victory for cybersecurity here and around the world.”

Bipartisan Group of Senators Introduce Internet of Things Bill

On Tuesday, a bipartisan group of senators introduced the Developing Innovation and Growing the Internet of Things (DIGIT) Act, which would establish a working group to examine how privacy and security should be protected in the Internet of Things. The group, which would include representatives from industry and government agencies (including the Transportation Department, the National Institute of Standards and Technology, and the Federal Communications Commission) would have one year to offer recommendations to the Senate Commerce and House Energy and Commerce committees. The bill is sponsored by Senators Deb Fischer (R-NE), Cory Booker (D-NJ), Kelly Ayotte (R-NH), and Brian Schatz (D-HI).

House Oversight Committee Approves Controversial Government Cybersecurity Bill

On Tuesday, the House Oversight Committee passed the Federal Information Systems Safeguards Act (H.R. 4361) out of committee by a vote of 21-16. The bill, introduced by Representative Gary Palmer (R-AL), would give agency heads “sole and exclusive authority,” with respect to IT or information systems under the agencies control, to “take any action the agency determines to be necessary to reduce or eliminate” current or future security weaknesses or risks.” The measure was sparked in part by disputes between federal employee unions and agencies over personal email use on government systems.

"In view of the breaches we have already experienced and the constant assault against our government information systems…the need of giving federal agencies the flexibility and authority to secure their third-party systems should be obvious," Rep. Palmer said, adding that "[i]t should also be obvious that to deny them this authority is to put America's information systems, and our federal employees, at greater risk.” However, the committee’s ranking member, Representative Elijah Cummings (D-MD), warned that the bill is “dangerously overbroad.” "This bill could open the door to

an agency violating other laws in the name of security," he said, asking whether “any action” could include ignore DHS directives on cybersecurity or violating the Privacy Act.

IRS Hacking and Identity Theft Woes Continue

Last Friday, February 26, the Internal Revenue Service (IRS) announced that the number of taxpayers whose personal data was compromised during last year’s attack on the “Get Transcript” service was closer to 720,000, more than double the previous announcement of 330,000. This is the second time the IRS has revised the estimate upward since first announcing the compromise in May. The IRS said it would begin mailing notifications to the additional identified taxpayers this week.

“The IRS is committed to protecting taxpayers on multiple fronts against tax-related identity theft, and these mailings are part of that effort,” IRS Commissioner John Koskinen said. The agency is offering victims an identity protection (IP) PIN as added security for this year’s tax filing, and a year of identity theft protection service. The IRS also said it will be sharing details of the Get Transcript hack with state revenue departments and members of the tax industry.

However, later this week, news began to come out that these new IP PINs had also been compromised, with the IRS having heard from at least a handful of taxpayer who had received IP PINs trying to file their taxes, only to be told that someone had already filed a. While Commissioner Koskinen said that this is a “relatively minor problem” affecting only a “handful” of filers, it may point to a more systemic issue. The problem: those who have been assigned IP PINs, by definition, have already been the victims of identity theft, making it easier for them to be re-victimized by using the PIN recovery function. If someone loses their IP PIN, the online tool to retrieve it only requires basic personal information and answers to “knowledge based authentication” questions—the same types of questions that were circumvented in the “Get Transcript” hack last year.

Upcoming Hearings of Note

- On Tuesday, March 8, the Senate Homeland Security Committee will hold a hearing on the President’s budget proposal for FY17 for DHS.