Cybersecurity: Washington Week in Review, Week of January 31

FEBRUARY 5, 2016

DHS Preparing to Share Cyber Indicators with Private Sector

On Tuesday, February 2, DHS Assistant Secretary for the Office of Cybersecurity and Communications Andy Ozment said that DHS will take steps this month to begin automatically sharing cyber threat information with private industry. DHS plans to start working with a small number of companies when it launches the initiative, in about two weeks, Ozment said. Ultimately, DHS plans to expand the program more broadly. “We want to live in a world where sharing indicators is like an immune system,” he said.

Ed CIO Grilled by House Panel

Danny Harris, Chief Information Officer for the Department of Education, faced an angry House Oversight Committee during a hearing on Tuesday. The hearing focused heavily on an IG investigation into Harris’s outside business activities, and the committee blamed such distractions for the agency’s lax computer defenses. “You’re a very, very busy man,” Representative Carolyn Maloney (D-NY) said, saying she “can understand why there are problems with cybersecurity at the Education Department when you have so many other outside jobs.”

"Mr. Harris has served as the chief information officer since 2008, and by virtually every metric he is failing to adequately secure the department's systems," Committee Chair Jason Chaffetz (R-UT) stated. Representative Chaffetz also noted that Harris had received over $200,000 in bonuses over the past decade, despite the Department’s performance deteriorating during last year’s “cybersecurity sprint.”

Harris acknowledged the department's lackluster performance, but insisted it is improving. And he said he was doing a better job with some of his other responsibilities. "One should look at the totality of my leadership, not just cyber," he said. Under fire, he acknowledged that his behavior was "unacceptable." His boss, acting Education Secretary John King, Jr, expressed confidence in Harris’s leadership. Following the hearing, Harris collapsed outside of the Rayburn House Office Building, though he was later reported to be conscious and in stable condition.

House Sends OPM Subpoena Day Before Confirmation Hearing

On Wednesday, February 3, the House Oversight Committee issued a subpoena to OPM for documents related to the breach, which the committee asked for months ago. “Despite assurances of cooperation, I'm disappointed [Acting OMB Director Beth] Cobert is not working in good faith with the Committee," Committee Chair Jason Chaffetz (R-UT) said. "We made a commitment to the American people to ensure a hack of this nature never happens again. The documents we've repeatedly requested be provided to this Committee are essential to fulfilling that promise."

The following day, Acting Director Cobert testified before the Senate Homeland Security Committee for her confirmation hearing. “We all think you're great," Chairman Ron Johnson (R-MN) told Cobert. "We want to see this nomination move forward." Senator Johnson told Politico that he would hold a vote next week on the nomination. But Republicans at the hearing questioned her over the House subpoena. "It's troubling they were forced to resort to a subpoena," Senator Johnson said. "I do that as a last resort." Cobert said she was reviewing the subpoena, and the agency is working “very actively” to respond to the requests.

White House Responds to House Letter on Export Control

On Tuesday, Representative Jim Langevin (D-RI) said that the only solution on the Wassenaar Arrangement’s language on cybersecurity products “may be to go back to Wassenaar and renegotiate." The comment was made in a press release announcing receipt of the White House’s response to the letter Representative Langevin organized from 125 lawmakers urging the National Security Council to become more involved in the interagency dispute on the issue. In the reply, Caroline Tess, Senior Director for Legislative Affairs for the National Security Council said that the administration promised to consider "the burden that such a rule may place on legitimate cybersecurity activities."

Clinton Comments on Cybersecurity While House Committee Investigates Recordkeeping

On Wednesday, Hillary Clinton said cybersecurity will have to be a top priority for the next president. “It’s one of the most important challenges the next president is going to face because the advances, the offensive advances by nation states that we know are very technically sophisticated—namely Russia, China, next level Iran, next level North Korea—are going to just accelerate,” she said during a town hall meeting in New Hampshire.

Unsurprisingly, these comments drew fire from the GOP in light of the ongoing investigation into Clinton’s use of a private email server while Secretary of State. "After setting up an unsecure email server in her basement that exposed highly classified information and triggered an FBI investigation, it goes without saying Hillary Clinton has flunked the cybersecurity test with flying colors," Michael Short, a Republican National Committee spokesman, said in an email.

Meanwhile, House Oversight Committee Chair Jason Chaffetz (R-UT) confirmed on Thursday, February 4, that his committee his moving forward with an investigation into federal recordkeeping practices, which is expected to focus heavily on Secretary Clinton’s emails. "Certainly the FBI, they should do their investigation," said Representative. Jim Jordan (R-OH), a member of the Oversight Committee who supports the new effort. The panel will look into how Clinton determined that only

roughly half of her 60,000 emails were work-related, he indicated, and will ask questions about the State Department's process for reviewing federal records.

IRS Failure Result of a Hack?

Late Wednesday night, a number of the IRS's tax processing systems went down due to technical problems, the IRS said. However, House Oversight Committee Chair Jason Chaffetz (R-UT) said that his "initial gut reaction" is that it may be a hack. "You just don't have systems collapse and people can't use the systems online," he added. "It's not like they run out of batteries or something. It really does smell like a hack."

Sector-Specific Updates:

- ***Defense.*** On Tuesday, Defense Secretary Ash Carter previewed DoD's spending plans, including plans to spend $7 billion on defensive and offensive cyber capabilities in 2017 and $35 billion over the next five years. This represents a 27% increase from the $5.5 billion DoD request in FY 2016.
- ***Energy.*** The Energy Policy Modernization Act (S. 2012), the Senate's energy reform bill includes a number of cybersecurity provisions, which supporters say will help bolster the power grid's cyber defenses. Senate Majority Leader Mitch McConnell (R-KY) applauded the cyber provisions on Tuesday while encouraging his colleagues to vote for the bill. Senator McConnell highlighted a number of the specific provisions, including one that authorizes additional cybersecurity research. Other clauses would also direct the agency to work more closely on fighting cyberattacks with other countries connected to the North American electrical grid. The bill, Senator McConnell said, "would help deter attacks by erecting stronger cybersecurity defenses, and it would help provide for faster and more effective responses when threats do arise
- ***Financial Services.*** This week, the Federal Deposit Insurance Corporation (FDIC) Division of Risk Management Supervision issued its Winter 2015 " Supervisory Insights," which discusses several topics, but leads with cyber, providing advise to banks to enhance their information security programs in response to increased cyber threats. The document's "Framework for Cybersecurity" covers a number of issues, including summaries of various types of threats, governance, and regulatory actions and resources.
- ***Government Agencies.*** Government officials have come to the defense of the government's main cyber defense system this week after a recent GAO report stated that, "[w]hile [its] ability to detect and prevent intrusions, analyze network data, and share information is useful, its capabilities are limited." Homeland Security Secretary Jeh Johnson said that the so-called "Einstein" program has considerably improved the government's ability to detect hackers, and has "in fact proven invaluable to identify significant incidents." However, he cautioned that the program is still in its final stages of implementation, and is not meant to be "a silver bullet." "It does not stop all attacks, nor is it intended to do so," he said. "It is part of a broader array of defenses." Michael Daniel, the president's cybersecurity coordinator, also defended the program. "I'm not going to argue that there aren't improvements that we can continue to make, but I think the core of the

technology is sound," he said. While Einstein is designed to scan traffic for threat signatures, newer systems focus on detecting anomalies indicative of an attack. However, Daniel noted that the signature-based approach remains valid, and that the key is to build on top of that, which is what DHS is working to do.