WILMERHALE

Cybersecurity: Washington Week in Review, Weeks of March 6 and 13

MARCH 18, 2016

SEC: More Cybersecurity Efforts on the Way?

Speaking at the Investment Company Institute's Mutual Funds and Investment Management Conference on Tuesday, March 15, Andrew Ceresney, head of the SEC's Enforcement Division, said that the Securities and Exchange Commission (SEC) has cyber enforcement actions "in the pipeline," saying that last years' action against R.T. Jones Capital "won't be the last case in this area."

During a speech at a Chamber of Commerce event on Wednesday, March 16, SEC Chair Mary Jo White said that, while the SEC is doing as much as its jurisdiction allows with respect to cybersecurity, especially for information-sharing and education, the government needs to have a clear plan in place for which government agencies will deal with which problems. "SEC is not going to be able to stop nation-state hacking," White said. "My concern is to make sure on the regulatory end, the government end, that you really have a very well understood plan for who does what."

She added that information-sharing has been particularly challenging, but that the SEC has tried to improve this with its Regulation SCI exams, which it uses to evaluate cyber trends and evolving risks in the financial services sector before publicly sharing its findings. White also noted that the SEC has made cybersecurity a high priority in its National Exam Program, focusing on cyber preparedness. She said the SEC is looking not only at firms' security systems, but also their responses to breaches and other incidents.

President Obama Tightens Sanctions on N. Korean Hackers

This Wednesday, President Obama issued an Executive Order tightening sanctions on North Korea. Among other things, the Executive Order imposes sanctions on "any person determined by the Secretary of Treasury, in consultation with the Secretary of State…to have engaged in significant activities undermining cybersecurity through the use of computer networks or systems against targets outside of North Korea on behalf of the Government of North Korea or the Workers' Party of Korea."

NIST Releases Draft BYOD Guidance

On Monday, March 14, the National Institute of Standards and Technology (NIST) released drafts of updated versions of two guidance documents related to teleworking, remote access, and "Bring Your Own Device" (BYOD) security: NIST Special Publications (SP) 800-46, "Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security," and NIST 800-114, "User's Guide to Telework and Bring Your Own Device (BYOD) Security." Comments are due by April 15.

DHS Releases Info-Sharing Privacy Impact Assessment, Begins Sharing Cyberthreat Information

This Tuesday, the Department of Homeland Security (DHS) released its privacy impact assessment for the cyberthreat information-sharing program under the Cybersecurity Information Sharing Act of 2015. According to the report, while there are safeguards to prevent personally identifiable information (PII) from being shared through the program, there is a "residual privacy risk that these processes may not always identify and remove unrelated [PII], thereby disseminating more [PII] than is directly related to the cybersecurity threat."

On Thursday, DHS announced that it had begun sharing information about cyberthreats with private entities under CISA. According to DHS, six entities have agreed to participate, and DHS Secretary Jeh Johnson explained that he is approaching industry-operated information sharing and analysis centers (ISACs) to participate in the new program.

Senators to Introduce State and Local Cyber Protection Act

Last Thursday, March 10, Senators Gary Peters (D-MI) and David Perdue (R-GA) announced that they will be introducing the State and Local Cyber Protection Act, a companion bill to one that passed the House in December. The bill is intended to increase information-sharing between DHS and state and local governments about cyber threats and vulnerabilities, including by requiring DHS to help state and local governments with tools, policies, procedures, technical assistance, and training. The legislation "will help ensure all levels of government are equipped with the best practices and resources to counter cyber threats," Senator Peters said in a statement.

Latest on IRS and OPM

Last Monday, the Internal Revenue Service (IRS) temporarily suspended its "identity protection" PIN program, citing ongoing security concerns. The announcement followed several reports of identity theft victims being revictimized by having their PIN numbers compromised. Later last week, the IRS said that it's seen a "surge" this year in phishing emails, with would-be identity thieves phishing payroll and HR employees in hopes of gaining access to companies' employees' personal information. Tax-season phishing attacks against individuals are also on the rise.

And from OPM, this Tuesday, Acting OPM Director Beth Cobert told the House Appropriations Committee subcommittee on financial services and general government that approximately 11% of OPM breach victims (2.5 million people) have signed up for the identity protection services offered by the agency in the wake of its breach. Cobert applauded the sign-up rate, which is significantly higher than the 2-3% of private sector data breach victims that typically enroll in these services.

Sector-Specific Updates

- ***Automotive.*** Senate Commerce Committee members used a hearing on self-driving cars on Tuesday to discuss whether such vehicles are vulnerable to hacking. “You can imagine in this world of cybersecurity and cyberattacks, imagine what would happen to autonomous vehicles to get hacked while they’re out on the road,” committee ranking member Bill Nelson (D-FL.) said. “One small defect could end up in a massive safety crisis.” Senators Ed Markey (D-MA) and Richard Blumenthal (D-CA), who have advocated mandatory data security standards, were the most vigorous in expressing their concerns. "Clearly hackers are going to have the ability to break into these vehicles,” Senator Markey said. “And so the kinds of protections you build in can be voluntary, but if 10 companies do it and 10 don’t, then those 10 are going to be identified by the hackers as the ones they’re going to be playing games with out on the highways.”
- ***Defense.*** Last Monday, the Department of Defense (DoD) released a long-awaited public version of its Cybersecurity Discipline Implementation Plan. The Plan, which was initially approved in October, includes discussion on authentication, device hardening, reducing the number of points available for attack, and aligning cybersecurity with compute network defense service providers. The Plan includes over three dozen security tasks for DoD components, along with criteria to assess completion.
- ***Financial Services.*** Last Tuesday, March 8, the Federal Deposit Insurance Corporation (FDIC) published a special issue of its quarterly consumer news alert entitled “A Bank Customer’s Guide to Cybersecurity.” The alert includes safety precautions for internet banking and shopping (including cybersecurity tips for small businesses), information on how to avoid identity theft online, and materials on what banks and bank regulators are doing to protect customers from cyberthreats. The FDIC also released brochures for individual and business bank customers. And this Tuesday, House Financial Services Committee Chair Jeb Hensarling (R-TX) said that his committee won’t move forward on legislation to increase regulation on online lenders and other fintech companies. While speaking at the annual American Bankers Association Summit, Representative Hensarling said that, while the committee is concerned about regulatory disadvantage for banks, he suggested that “the answer is not necessarily to bring them down but to bring you up.”
- ***Healthcare.*** On Wednesday, the Department of Health and Human Services (HHS) announced the members of the Health Care Industry Cybersecurity Task Force, established pursuant to the Cybersecurity Act of 2015. Members represent a variety of organizations in the healthcare and public sectors, including insurers, hospitals, patient advocates, security researchers, pharmaceutical companies, medical device manufacturers, health IT vendors, laboratories and government agencies. The Task Force will hold four public meetings this year. The announcement notes that the Task Force expects to deliver its report by next March. Meanwhile, early last week, HHS released an audit by E&Y, which found that the agency had made progress implementing cybersecurity protections to conform with the Federal Information Security Modernization Act, though there was still room for improvement.

Upcoming Hearings of Note

- On Tuesday, March 22, the House Homeland Security Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies will hold a hearing on the role of cyber insurance in risk management.
- On March 22, the House Armed Services Subcommittee on Emerging Threats and Capabilities will hold a hearing on FY17 IT and cyber programs