Cybersecurity: Washington Week in Review, Weeks of March 20, 27 and April 3

APRIL 8, 2016

Homeland Security Committee and DHS Review Cyber Insurance Market

On Tuesday, March 22, a House Homeland Security subcommittee held a hearing on the Role of Cyber Insurance in Risk Management. In advance of the hearing, Subcommittee Chair John Ratcliffe (R-TX) said that the purpose of the hearing was to introduce the topic, and that he isn’t looking toward a legislative solution soon. But he wanted to understand whether the state of cyber insurance is an impediment to good cyber hygiene and, depending on the answer, whether cyber insurance can be a driver of better hygiene going forward (similar to how homeowners’ policies give incentives for homeowners to buy smoke detectors).

At the hearing, witnesses and lawmakers warned that the market might take decades to mature, and hesitated to pin down a clear role for the government. "Security dollars are finite, and companies are assessing, would they rather spend another dollar on a technical solution or put that dollar toward insurance?" Matthew McCabe, senior advisory specialist on cyber insurance at the brokerage Marsh LLC, said at the hearing. "Companies would prefer technical solutions, but over time we learn there's no silver bullet." But, said Daniel Nutkis, CEO of the Health Information Trust Alliance, companies are beginning to realize that improving their cyber defenses lowers insurance costs.

Adam Hamm, testifying for the National Association of Insurance Commissioners, cautioned that the cyber insurance market "is in its infancy." "What this market really needs is time, patience and support," he said. He suggested government could help develop the supply of actuarial data, though that might grow "organically over time." But Hamm said the federal government is not his preferred outlet for centralized actuarial data.

Shortly after the hearing, on Monday, March 28, DHS published a notice seeking comments on three white papers regarding cyber insurance and risk management, and how DHS can play a role in this by potentially developing a cyber incident data repository.

President Obama Renews Cyber Sanctions Authority

On Tuesday, March 29, President Obama sent a notice to Congress extending the “national emergency...with respect to significant malicious cyber-enabled activities” described in his April 2015 cyber sanctions executive order, thereby renewing the authority for the order. While the White House has yet to use this authority, the rumored threat of its use was a potentially significant source of negotiating leverage in advance of last year’s cyber pact with China.

Obama Administration Blames Iran for Dam Attack

On Thursday, March 24, the Justice Department unveiled an indictment against seven hackers tied to the Iranian government, accusing them of mounting "a coordinated cyber assault" on 46 US banks and other financial institutions from 2011 to 2013, and trying to take control of a small dam in New York. While only unsealed now, the indictment was returned in late January, just a few days after the US and Iran implemented the recent nuclear deal.

"If hackers are able to access dams, the electrical grid, airports, our water supply or nuclear plants, the amount of damage they could do is enormous," Senator Dianne Feinstein (D-CA) said after the indictments were unsealed. Senator Chuck Schumer (D-NY) said the indictments show that the U.S. "must step up our counter-hacking game ASAP.” Representative Adam Schiff (D-CA) described the indictments as a "warning to U.S. companies and individuals that the threats we face online are pervasive and potentially devastating." Other lawmakers, however, wanted more to be done. Representative Jim Langevin (D-RI), co-chair of the Congressional Cybersecurity Caucus, suggested that the White House should consider blocking the hackers’ assets using the cyber sanction authority.

In the wake of the indictments, on Wednesday, April 6, Senator Mike Rounds (R-SD) introduced the Iran Cyber Sanctions Act, a bill that would direct the White House to prepare a report on Iran’s efforts to launch cyber attacks against US government and corporate interests, and sanction individuals identified in the report.

Senate Passes Trade Secrets Act, House Readying to Move

On Monday, April 4, the Senate passed the Defend Trade Secrets Act (S. 1890), which would allow companies to sue trade secret thieves in federal court. Senators Orrin Hatch (R-UT) and Chris Coons (D-DE), the bill’s cosponsors, said their bill would harmonize federal law and give businesses more consistent legal protections when their trade secrets are stolen and they are facing billions in losses. Speaking on the Senate floor before the vote, Senator Hatch said the bill required two years of work and "much effort not only to identify the precise nature of the problem - a problem that amounts to hundreds of billions of dollars in economic loss for US companies annually—but also to develop a solution that could garner the support of virtually all stakeholders." He noted that the measure is widely supported, adding that "the final version of the legislation...reflects input and additions from a broad coalition of interested parties."

The bill, which is seen as an important tool for companies to go after insider data security threats, passed with an 87-0 vote. Following the Senate vote, House Judiciary Committee chair Bob Goodlatte (R-VA) said he plans to move the House’s version of the bill.

GAO, Congress Express Concerns Over Federal Protection of Taxpayers’ Info

According to a GAO report released on March 28, the IRS has made some progress on improving data security, but has significant room for improvement. The report found that the agency did not always implement effective controls regarding user authentication, did not ensure sensitive user information was encrypted, and exposed the IRS to known vulnerabilities due to unpatched and outdated software. According to the report, several problems stemmed from inconsistent implementation of the agency's information security program. The IRS also failed to effectively correct nine of the 28 previously identified weaknesses the agency claimed to have addressed.

Unless the IRS "takes additional steps to address unresolved and newly identified" problems with its security controls, and updates its policies and testing procedures, the report concluded, "taxpayer data will remain unnecessarily vulnerable to inappropriate and undetected use, modification, or disclosure."

Following the report's release, House Speaker Paul Ryan (R-WI) posted a statement to his website, urging the IRS to immediately adopt reforms to protect taxpayer information. "Right now, as you're sending the IRS just about everything there is to know about you, it remains highly vulnerable to hackers and cyberattacks. And the agency has no intention of doing anything about it," the statement from Speaker Ryan's communications director, Michael Shapiro, states. The statement describes the IRS's response to the report as "[t]he usual excuses and evasions," and says that "'[w]e'll think about it' isn't good enough."

Shortly before the release of the report, House Oversight Committee Chair Jason Chaffetz (R-UT) sent a letter to the GAO, asking GAO to study how agencies have reduced their reliance on Social Security numbers in light of their increased use for identity theft.

Sector-Specific Updates

- ***Aviation.*** On Thursday, April 7, Senator Ed Markey (D-MA) introduced the Cybersecurity Standards for Aircraft to Improve Resilience Act of 2016 (the Cyber AIR Act), a proposed amendment to the FAA authorization bill, which would require the FAA to establish cybersecurity standards and require airlines to disclose cyberattacks to the federal government. The amendment would also require further studying on the cybersecurity vulnerabilities of passenger use of WiFi, and would direct the FAA to integrate cybersecurity measures into the air traffic control system.
- ***Defense.*** On Friday, March 25, the Defense Information Systems Agency released an update to the Cloud Computing Security Requirements Guide (SRG), the security requirements applicable under new DoD rules to contractors offering cloud services to DoD.
- ***Energy.*** In the wake of a December cyber attack against the Ukrainian power grid, the North American Electric Reliability Corporation (NERC), in conjunction with SANS, issued a series of recommendations detailing how to improve protection for electric substations.
- ***Financial Services.*** On Thursday, March 31, Treasury Deputy Secretary Sarah Bloom Raskin spoke at the inaugural Incident Response Forum, focusing on public/private coordination in response and recovery efforts in the financial services sector.

- ***Government Agencies.*** According to OMB's annual report under the Federal Information Security Modernization Act (FISMA), released on Friday, March 18, federal government agencies were subject to more than 77,000 "cyber incidents" in FY 2015, a 10% increase over FY 2014. According to the report, some of the increase is a result of an improved capability to detect the incidents. The OMB report gave federal agencies an overall FISMA compliance score of 68 out of 100, an 8% decrease year-over-year. OMB says the drop reflects a more thorough scoring methodology. Others, however, point to a decline from 92% to 57% for the Department of Interior, which houses OPM personnel records, as a significant source of the decline.
- ***Healthcare.*** On Monday, March 21, HHS announced that it will launch long-anticipated audits to assess compliance with the Health Insurance Portability and Accountability Act (HIPAA). HHS's Office of Civil Rights (OCR) will collect pre-audit information from HIPAA "covered entities" and "business associates," and, from there, will develop a pool of approximately 200 audit targets for a mix of "desk audits" and in-person audits. If an audit turns up a "serious compliance issue," OCR said, further investigation could result in financial penalties and a formal agreement to improve HIPAA compliance. HHS will also use findings to develop guidance and policies to strengthen HIPAA compliance. Following the announcement, on Wednesday, March 6, Deven McGraw, deputy director for health privacy at OCR, said health providers are failing at "Security 101," saying that many do not understand the basics of protecting information. McGraw was particularly annoyed by the number of breaches resulting from the theft or loss of an unsecured laptop.

Upcoming Hearings of Note

- On April 12, the Senate Finance Committee will hold a hearing on cybersecurity and protecting taxpayer information.
- On April 14, the House Transportation Subcommittee on Economic Development, Public Buildings and Emergency Management will hold a hearing entitled "Blackout! Are We Prepared to Manage the Aftermath of a Cyber-Attack or Other Failure of the Electrical Grid?"
- On April 14, the House Science, Space, and Technology Subcommittee on Research and Technology will hold a hearing examining whether the IRS can protect taxpayers personal information.