ML STRATEGIES

#MLWashingtonCyberWatch: The Cybersecurity Executive Order (at last)

May 18, 2017 | | By **Cynthia J. Larose**, Joanne Dynak, Michael Katz

Amid the flurry following former FBI Director James Comey's firing last week, President Trump marked his 111th day in office on Thursday, May 11th by signing an executive order targeting national cybersecurity.

The long-awaited order is the first step in fulfilling Trump's promise to address national cybersecurity concerns and it arrives as threats of international hacking and cyberattacks reach an all-time high. It establishes three overarching cybersecurity priorities for the United States: (1) protecting federal networks, (2) reinforcing critical IT infrastructure, and (3) protecting the American public in the online space. The full text of the executive order can be found here.

While the order includes few actionable items, it sets strict deadlines for government agencies to produce risk reports and recommendations for improving their data security practices, signifying an important call to action from the executive branch that places risk management at the forefront.

Modernizing & consolidating federal networks

Consolidating to the cloud will likely be the first major step toward overhauling the government's administration-wide cybersecurity protocol. In a press briefing last Thursday, White House Homeland Security Advisor Tom Bossert addressed what he views as fractured, agency-specific IT security practices across the government, noting that "[if] we don't move to shared services, we have 190 agencies all trying to develop their own defenses against advanced collection efforts."

The move to modernize is an extension of similar efforts from the Obama administration to bolster cybersecurity, an area in which Bossert says the administration made "**a lot of progress … [but] not enough**." In line with advancing these efforts, the executive order requires federal agencies to use the **Framework for Improving Critical Infrastructure Cybersecurity** developed in 2014 by the National Institute of Standards and Technology ("NIST") to manage cybersecurity risk. Coincidentally, the Framework may be **revised soon as the NIST recently closed a comment period on an updated draft** that it circulated in January 2017, and per the executive order any successor document to the Framework will become the operative version to be used by government agencies. Separately, Rep. Will Hurd (R-TX), Chairman of the House Information Technology Subcommittee, **recently reintroduced H.R. 2227, the "Modernizing Government Technology Act,"** which secures more efficient funding for the modernization of federal IT infrastructure and is expected to hit the floor of the House of Representatives within the next couple of weeks.

Reinforcing critical infrastructure

The second prong of the executive order requires the Secretary of Homeland Security to prepare an audit of potential vulnerabilities across the country's infrastructure systems – from financial and telecommunications systems to utilities including water and electricity. Improving transparency about the security gaps in these systems is crucial, especially as **traditional data breaches** are losing ground to more devastating Distributed Denial of Service (DDoS) botnet attacks made possible by the growing Internet of Things, or "IoT" (see our blog post **here** for a discussion of the House's efforts to address growing security concerns around the IoT).

Protecting the public online

Finally, President Trump's executive order urges policies aimed at protecting U.S. citizens from domestic and foreign online threats. In addition to increasing the number of cybersecurity experts working with the White House, Bossert suggested that following through on such policies will require greater partnerships between the federal government and the private sector. Indeed, the government currently relies on technology from large, long-time vendors, **many of which may not be prepared to grapple with the significant and evolving risks becoming apparent across the data security landscape**. Independent technology startups are proving to be the heart of progress in new cybersecurity measures, and the government will need to cultivate solid relationships with these players if it wants to **stay ahead in the cybersecurity arena**.

President Trump's executive order has received some criticism for its breadth, but overall has been commended by cybersecurity experts as a balanced step in the right direction. Time will tell whether the

resulting policies will make a meaningful difference in the country's ability to fend off attackers in the ever-evolving online battleground.

Authors

Cynthia Larose

Joanne Dynak

Michael Katz