Obama signs executive order on sharing cybersecurity threat information

February 13, 2015

PALO ALTO, Calif. — President Barack Obama signed an executive order Friday that urges companies to share cybersecurity-threat information with one another and the federal government.

Obama signed the order, which is advisory in nature, at the first White House summit on Cybersecurity and Consumer Protection at Stanford University here. The summit, which focused on public-private partnerships and consumer protection, is part of a recent White House push to focus on cybersecurity.

Obama said the prospect of cyberattacks are one of the nation's most pressing national security, economic and safety issues. The specter of a cyberattack crippling the nation's air traffic control system or a city with a blackout is real, and hacks such as the one on Sony Pictures last year are "hurting America's companies and costing American jobs." He also said they are a threat to the security and well-being of children who are online.

"It's one of the great paradoxes of our time that the very technologies that empower us to do great good can also be used to undermine us and inflict great harm," Obama said before a cheering, friendly audience here at Stanford's Memorial Auditorium.

The order encourages the development of central clearinghouses for companies and the government to share data and creation of centers where data can be shared across specific geographic regions.

"There's only one way to defend America from these cyber threats, and that is through government and industry working together, sharing appropriate information as true partners," he said.

The order is part of a broader White House effort to beef up the nation's cybersecurity infrastructure, something the administration wants to push on Capitol Hill. Last month Obama proposed legislation that would shield companies from lawsuits for sharing threat data with the government.

Obama has signed other executive orders, including one that calls for the creation of voluntary standards to bolster the security of computer networks in critical industries and a framework for cybersecurity and another last year to protect consumers from identity theft. So far nothing has

been able to stem the tide of attacks such as the one against Sony or others against retailers including Home Depot.

Both privacy groups and Silicon Valley companies have said they would oppose the legislation Obama proposed last month unless reforms are first made to the NSA's surveillance program.

U.S. government surveillance activities have been seen as a potential liability for tech companies that operate globally.

"Seventy to 80 percent of the user bases for a lot of these companies are the foreigners who get very little protection under our system," explained Julian Sanchez, a senior fellow focused on technology and civil liberties at the Cato Institute. "If they don't display some push back, they know they won't do very well with those markets."

In December of 2013, major tech companies including Apple, Google, Twitter, Facebook, Microsoft and Yahoo joined together in the Reform Government Surveillance coalition, urging the president and Congress to impose restrictions and oversight measures on U.S. spying programs.

The president agreed in principle to some limits on spying programs, including the bulk collection of domestic phone records, during a speech last year. But progress on reforms has been too slow for some privacy advocates, as the administration urged for legislative action that has yet to succeed.

Tech companies, meanwhile, have taken some measures into their own hands by strengthening and expanding their deployment of encryption to secure users' online activities — setting up a conflict between the companies and law enforcement who warn that such actions may make it harder for them to pursue crime and terrorism which increasingly includes a digital component.

"I think it's fair to say that changes on the technology front have outpaced governmental and legislative efforts," said Andrew Crocker, a legal fellow at civil liberties group the Electronic Frontier Foundation.

Sen. Tom Carper, D-Del., earlier this week introduced cyber-threat and intelligence-sharing legislation that mirrors many of the recommendations from the White House's proposal.