MIT Technology Review

Why Obama's Cyber Defense Order Won't Amount to Much

The president's executive order falls short of meeting the severity of the cyberattack threat.

By David Talbot on February 15, 2013

There's been a lot of rhetoric recently about the threat that cyberattacks pose to national infrastructure, but President Obama's new executive order – with its focus on voluntary standards and information sharing – is unlikely to provide much protection. The executive order requires that new information-sharing, standards-setting, and R&D plans get up and running over the next few months to two years.

Attacks on government agencies and infrastructure are apparently on the rise. Breaches reported to the U.S. Department of Homeland Security's cyber security response team grew 52 percent to 198 attacks in 2012 (see "Old Fashioned Control Systems Make U.S. Power Grids, Water Plants a Hacking Target"). Meanwhile, malware writing has become a huge industry, supported by governments and defense contractors as well as criminals (see "Welcome to the Malware Industrial Complex"). The president has called cyber threats "one of the most serious economic and national security challenges" facing the nation.

The executive order – announced during Obama's State of the Union address – won't force companies to introduce measures that would protect infrastructure like the power grid. Ravi Sandhu, executive director at the Institute for Cyber Security at the University of Texas at San Antonio, says this seriously limits its value. "This sounds like a strategy of: 'Let's keep trying the same thing again, and maybe this time is it will succeed,' or perhaps kick the can down the road so it becomes someone else's problem," he says. "I don't see much chance of meaningful success. Cybersecurity of critical infrastructure should be a high priority for all nations."

Among other things, the Executive Order Improving Critical Infrastructure Cybersecurity tells the National Institutes of Standards and Technology to create a security framework that private companies that operate critical infrastructure could voluntarily follow.

Stewart Baker, a consultant who was the former general counsel at the National Security Agency and policy chief at the Department of Homeland Security during parts of the second Bush administration, says that's a good start, but it will be prone to lobbying influence. Defining the framework may be "so encumbered by political correctness, fear of imposing costly burdens, and procedural requirements that it will take many years to complete, by which time all of the security measures will be out of date, leaving us no better protected than before," he says.

Much of the nation's information technology infrastructure is owned by private companies, making efforts by those companies crucial to national security. However, while the order beefs up how federal agencies share unclassified information with companies, it doesn't require companies to share their own attack information and intelligence with the government, though in practice many companies do this (see "Obama Announces Plan to Shore up U.S. Cyber Defenses").

A bill that passed the House last year and was reintroduced this week, called the Cyber Intelligence Sharing and Protection Act, or CISPA, would require companies to share more information, but it has been attacked by privacy and civil liberties groups who say it would encourage companies to hand over too much personal Internet data to government and security agencies. The American Civil Liberties Union praised the executive order and blasted the CISPA effort, suggesting that the privacy concerns were substantial. Obama took a similar position last year in opposing the CISPA bill. It was one of about 80 bills that touched on cybersecurity in recent years, none of which became law.

Whatever standards emerge, the fact that they'll be voluntary is not a fatal flaw, Baker says. Companies that don't follow them could face a competitive or public relations disadvantage, or a higher risk of litigation, he says: "Following government standards is a good way to rebut claims of negligence." One advantage of the order is that it requires the government to clean up its act by sharing information more seamlessly across agencies. Many agencies have cybersecurity research and development going on – and some of this work is redundant or hobbled by a lack of coöperation, says Radu Sion, a computer scientist at Stony Brook University and a leader in cloud computing security research. "The opportunity to finally synchronize federal efforts ... as well as the proposed individual elements can be of significant impact," he says.

Left unspoken in the president's order was the parallel effort by the federal government to develop offensive cyber weapon capabilities – which many see as more effective in preventing attacks than simply shoring up defense, at least when the attacker is state-sponsored (see "Should We Fire the First Shot in a Cyberwar?").

Tagged: Computing, Communications, Web, cybersecurity, state of the union, critical infrastructure