Obama executive order could be important in fight against computer attackers

February 13, 2013

Computer attacks have become so frequent and dangerous that the government needs help from private sector companies to protect information and infrastructure, U.S. Attorney for Western Pennsylvania David Hickton told the Tribune-Review.

The cybersecurity executive order that President Obama signed into law on Tuesday and mentioned in his State of the Union address can be an important tool in that fight against computer attackers by encouraging communication and cooperation between the government and private sector companies, Hickton said.

"I regard the cyber threat as a top present threat and the primary future threat in terms of national security and preventing the piracy of business capital and trade secrets and the individual identities of our citizens," Hickton said. "It's so serious that it cannot be dealt with by government alone." The executive order requires the government to share computer threat information with companies and to set voluntary guidelines for key industries that could be targeted by hackers, such as banking and transportation. The National Institute of Standards and Technology will create a list of computer security practices to reduce threats to critical infrastructure, such as energy companies that oversee the nation's power grid.

The Trib reported on Sunday in its ongoing "Cyber Rattling: The Next Threat" series how online attacks, such as recent ones against PNC Bank and other U.S. banks, are part of an ongoing international war over information systems. Attackers are becoming more sophisticated as they seek to create destructive computer incidents.

"It would be very difficult for the government on its own to really combat and prevent cyber attacks from happening both to the government and to the private sector," said Keith Tagliaferri, senior vice president of operations at Tiversa, a Downtown-based information security company.

"There is a mandated give-and-take that has to take place," Marty Lindner, principal engineer at CERT, a CMU program that works with the military, agreed. "From a technical perspective, both sides have something to bring to the table. If we want to

improve cybersecurity, we need to figure out better ways of sharing and coordinating activities." The president's executive order does not go as far as failed legislation last year opposed by the U.S. Chamber of Commerce and business leaders concerned about overreach by the federal government. Lawmakers of both parties said they would reintroduce a version of that bill on Wednesday, and the House Intelligence Committee plans to conduct a hearing on the topic on Thursday.

Critics said they worry the executive order still could lead to over-regulation, higher costs and increased corporate liabilities.

"I'm afraid that it's going to be a harbinger for government regulation of the 'network,' " said Paul Rozenweig, a visiting fellow at the Heritage Foundation conservative think-tank and a former deputy assistant secretary for policy in the Department of Homeland Security.

The private sector should be left to figure out computer security on its own with market forces determining what works, said Jim Harper, director of information policy studies at The Cato Institute, a think-tank that supports limited government.

Others counter that government already has played a key role in protecting some industries, such as banking and investing, from damaging attacks.

"I know we say, 'All of a sudden big, bad government is showing up here,' but in many ways, it's already involved at some level," said Tony Busseri, CEO of Route1, a Washington-based information security contractor.

Even before last fall when PNC Bank started suffering so-called "denial of service" attacks that prevented some customers from accessing online accounts, the company had been working quietly with government investigators to thwart attacks, said Hickton, who made computer security a top priority when he reorganized the U.S. Attorney's Office in 2010.

A PNC spokeswoman declined to comment on Tuesday.

Victims of computer hacking often are reluctant to admit they have been compromised because it might make them seem vulnerable or open them up to more attacks, Hickton said. But the government can make companies aware of vulnerabilities, provide access to government resources and educate them on ways to protect themselves.

"I can say on behalf of the administration that we're mindful of the concerns of private industry," Hickton said. "We have no desire to misuse our partnerships with the private sector." Andrew Conte is a staff writer for Trib Total Media. He can be reached at 412-320-7835 or andrewconte@tribweb.com.