Partners: Obama's Sanctions vs. Cyberattacks Is Step In Right Direction

Leveling sanctions against cyberattackers -- a move authorized Wednesday by President Barack Obama via executive order -- is a small step in the right direction, solution providers said. But as security breaches have become more prevalent, they warned that more must be done to address the mounting security threat.

The executive order declares a national emergency and authorizes "targeted sanctions against individuals or entities whose actions in cyberspace result in significant threats to the national security, foreign policy, economic health or financial stability of the United States," according to a blog post written by the president about the order. Those threats could include damaging infrastructure or networks and stealing personal information or company trade secrets.

"As Americans, our security, prosperity, and privacy in the 21st century will depend on our ability to learn, innovate, build and do business online -- and do it safely, knowing that our sensitive or personal information will be protected. As of today, the United States has a new tool to protect our nation, our companies, and our citizens -- and in the days and years ahead, we will use it," Obama wrote in the post.

The order gives the Treasury secretary, working with the attorney general and the secretary of state, the authority to take concrete action to prevent such attacks, including freezing assets, making it more difficult for the attacker to do business in the U.S. and cutting back on the attacker's ability to profit from cyberattacks.

The news comes in the midst of a barrage of recent high-profile cyberattacks, including the data breach of Sony Pictures by North Korea late last year. For those reasons, Obama said in his blog post, overseas cyberthreats would be the organization's first priority, bringing together targeted sanctions with diplomatic and law-enforcement tools.

Solution providers said that they saw the move as a progressive step in the fight against cyberattacks, but warned that this executive order can't be the be-all, end-all when it comes to government actions against security threats.

"We would definitely like to see those people prosecuted and 'hung in the central square' ... as a deterrent for others to stop doing that," said Steve Pearce, chief technology officer at

Houston-based ERGOS Technology Partners, adding that a few of his clients have been the victims of cyberattacks.

While Obama plans to target overseas cybercriminals, ERGOS' Pearce said he doubts the administration will be able to keep up with the scale and breadth of the "cat and mouse" game of international incursions.

"I don't think Obama has any chance of making a dent in what's happening, because most of those attacks are happening overseas," Pearce said.

Sebastian Lagana, senior analyst at Hampton, N.H.-based Technology Business Research, said he sees the executive order as having the right intentions, but worries it won't have the "teeth" it needs to create progress.

"I think it's a good start," Lagana said. "I think it's a good platform off which to build, but as currently constituted ... I think it's a lot more media fodder and awareness-generation than it is a bill with teeth that will require significant change in the short term."

Alexander Muchnik, technical engagement manager at Fort Lauderdale, Fla.-based **JDL Technologies**, agreed, saying that the executive order will help deter some companies, but won't solve the problem entirely.

"Threats to our cybersecurity are with us to stay, and I don't think anyone would argue with that," Muchnik said. "We believe that the new targeted sanctions will help to deter some cybercriminals, and perhaps the threat of sanctions will inspire some curtailment of these threats. The challenge, as it often is, will be to put teeth into the sanctions and walk the walk, now that we've talked the talk."

Part of the larger challenge, Lagana said, is that in order to fully address these security issues, both the federal government and commercial companies are going to need to step up their game and upgrade to more secure underlying infrastructure.

The challenge with that, Muchnik said, is that it requires commitment from all levels of the organization, as a network can be infiltrated by the "simplest of actions, or failures to act," such as missed patches or a failure to proactively monitor networks 24/7.

"While our government is taking the actions that it has the power to take, our corporations and businesses need to exercise the same vigilance. In the final analysis, security is everyone's responsibility," Muchnik said.

Sarah Kuranda's article was posted on April 1, 2015 at:
http://www.crn.com/news/security/300076363/partners-obamas-sanctions-vs-cyberattacks-is-step-in-right-direction.htm