CARLTON FIELDS

Cyberspace Developments: Obama's Proposed Information-Sharing Bill

CYBERSECURITY AND PRIVACY | INTELLECTUAL PROPERTY | JANUARY 15, 2015

Steven Blickensderfer

In advance of the State of the Union address, President Obama unveiled the next steps in his plan to address recent threats by rogue hackers to public and private networks. These include a new legislative proposal to tackle the information-sharing challenges that can cripple cyberattack responses, and revisions to those provisions of the 2011 legislative proposal on which Congress has yet to act.

The release of this strategy is a significant development in the cybersecurity space. It demonstrates that the White House and Congress are preparing for increased regulation and legislation in this area, going beyond the steps states have already taken. U.S. companies should begin to prepare for increased oversight, regulatory requirements, and enforcement efforts by the federal government on all cybersecurity and information management matters.

The proposed bill codifies mechanisms for enabling cybersecurity information-sharing between private and government entities, and among private entities. The key provisions include:

- Private companies whose customer data is breached must inform affected individuals within 30 days.
- Companies would be further encouraged to share cyberthreat information with the Department of Homeland Security's National Cybersecurity and Communications Integration Center, which, in turn, would share the information with other government agencies and industry groups known as Information Sharing and Analysis Organizations (ISAOs) that are being formed to help monitor and disrupt attacks.
- Companies that share cyberthreat information would get liability protection for sharing the information, as long as steps are taken to protect consumers' personal information.

The proposed bill also aims to modernize law enforcement authorities to combat cybercrime. The key criminal provisions include:

- Update the Racketeering Influenced and Corrupt Organizations Act (RICO) to apply to cybercrimes.
- Allow for the prosecution of the sale of botnets, computer networks created to carry out cybercrime, and give courts authority to shut down botnets involved in denial of service (DOS) attacks and other fraudulent activity.
- Criminalize the overseas sale of stolen financial information.
- Expand federal law enforcement to deter the sale of spyware used to stalk or commit identity theft.
- Update the Computer Fraud and Abuse Act to make clear it can be used to prosecute insiders who abuse their ability to access information.