PROTIVITI FLASH REPORT

Proposed Cybersecurity Information Sharing Act Sparks Controversy

October 26, 2015

The Cybersecurity Information Sharing Act (CISA) is a proposed law intended to improve cybersecurity in the United States through enhanced sharing of information about cybersecurity threats, and for other purposes. Introduced last year, the bill is currently under consideration in the U.S. Senate and faces an imminent vote. This Flash Report discusses some of the particulars of the bill and the controversy it has spawned.

Background

Now out of committee (via a 12-3 vote by the Senate Intelligence Committee) and potentially up for a floor vote very soon, CISA would allow (but not require) the sharing of Internet traffic information between U.S. government agencies and technology and manufacturing companies, making it easier for companies to share cyber threat information with the government. Specifically, the bill directs the Director of National Intelligence (DNI), the Department of Homeland Security (DHS), the Department of Defense (DOD), and the Department of Justice (DOJ) to develop and promulgate procedures to promote:

- The timely sharing of classified and declassified cyber threat indicators in possession of the federal government with private entities, non-federal government agencies, or state, tribal, or local governments;
- The sharing of unclassified indicators with the public; and
- The sharing of cybersecurity threats with entities to prevent or mitigate adverse effects.

The bill provides legal immunity from privacy and antitrust laws to companies which provide threat information (e.g., from private communications of users) to appropriate federal agencies and with other companies. It also permits private entities to monitor and operate defensive countermeasures to detect, prevent, or mitigate cybersecurity threats or security vulnerabilities on their own information systems and, with authorization and written consent, the information systems of other private or government entities. Therefore, private entities would be authorized to monitor information that is stored on, processed by, or transiting their systems.

With respect to privacy, the bill includes provisions for preventing the act of sharing data known to be both personally identifiable and irrelevant to cybersecurity. Therefore, any personal information or specific persons not directly related to a cybersecurity threat must be removed prior to sharing threat indicators or defensive measures. The bill directs the DOJ to develop, and make publicly available, guidelines to assist entities in sharing indicators with the federal government, including guidance for identifying and protecting personal information.

In essence, the bill creates a system for federal agencies and, in some cases, the intelligence community to receive threat information from private companies in which the submitting

companies are not required to obtain a warrant to submit such information to the government. It also offers a framework for the sharing of cybersecurity threat data between companies. Shared cyber threat indicators can then be used to prosecute cybercrimes, but may also be used as evidence for crimes involving physical force. For example, private communications between U.S. citizens and known terrorist groups would likely fall within the proposed bill's scope.

The bill follows up on recently passed cybersecurity legislation passed in the House of Representatives.[1] If passed in the Senate, the bill would then go into conference in which a handful of members from the Senate and the House are appointed to serve on a committee to address the differences between the two bills and work out a compromise bill. This exercise will be difficult as there are presently significant differences in the two bills. If a compromise bill is formulated and passed in both the House and the Senate, it will go to President Obama for his formal approval or veto.

While the president is on record supporting information-sharing legislation, he has not stated a specific position on the Senate's proposed bill. That said, the White House has stated in the past that any bill submitted for approval must protect the privacy of Americans.[2]

Proponents and Opponents

Everyone who reads the newspapers knows of the unique threats facing the free world and how perpetrators of those threats are using the Internet as a tool to find new recruits and motivate them to commit violent crimes. Some perpetrators of violent crimes may even tip their intentions to commit those crimes through social media. The question arises as to whether the appropriate authorities should be tipped when such information is discovered. Then there is cyber espionage, which is damaging the country. With these things considered, it is understandable why the CISA proponents argue the need for such legislation due to its worthwhile goal of protecting the citizens and crown jewel information assets of the United States.

The question raised by opponents of CISA centers around whether it offers the right approach. For example, does Congress understand the issues posed by CISA? Will a one-size-fits-all framework for information sharing work for every situation? Will the bill's approach unnecessarily expose personally identifiable information (PII) to government agencies that have been unsuccessful in protecting that information in the past? Will private companies be encouraged to submit significant amounts of personal customer data? What does "encourage" really mean and does it open up the potential for governmental coercion? Are further amendments to the bill needed to narrow the scope and depth of the information being collected and used by federal agencies? These are just a few of the questions being raised.

The United States Chamber of Commerce, National Cable & Telecommunications Association and other advocacy groups have gone on record in support of CISA in its present form. These proponents assert that sensitive information is already flowing freely out of our borders to the spies and criminals around the world.[3] The Computer & Communications Industry Association and notable technology companies oppose CISA, as do civil liberties groups advocating Internet privacy. These opponents assert that the bill gives companies license to spy on potentially

[1] The United States House of Representatives passed the Cyber Intelligence Sharing and Protection Act (CISPA), with amendments, in April 2013.

[2] "The Big One: Time Is Running Out on Major Cybersecurity Bill," Chris Bing, DCInno, August 8, 2015.

[3] See www.uschamber.com/sites/default/files/documents/files/10.19.15_coalition_s754_cisa_senate.pdf for letter from "The Protecting America's Cyber Networks Coalition" to the members of the United States Senate.

innocent people and will needlessly expose PII.[4] Even within the Senate itself, the proposed bill has bipartisan support as well as bipartisan opposition.

Summary

The fundamental issues with CISA are trust and concerns with privacy. The repeated high profile security breaches of PII and other sensitive data have led to people no longer trusting the capabilities of the government and large corporations with securing their data. It is interesting that the Department of Homeland Security, which has been designated the entry point for all submitted data so it can scrub it before it is disseminated, opposes the bill. Furthermore, there is the common criticism that CISA is privacy-invasive and opens the door to abuse.

Please note that this information is not intended to be legal analysis or advice, nor does it purport to address every issue that may impact financial institutions and other companies or every government response. Organizations should seek the advice of legal counsel or other appropriate advisers on specific questions as they relate to their unique circumstances.

About Protiviti

Protiviti (www.protiviti.com) is a global consulting firm that helps companies solve problems in finance, technology, operations, governance, risk and internal audit, and has served more than 60 percent of *Fortune* 1000® and 35 percent of *Fortune* Global 500® companies. Protiviti and our independently owned Member Firms serve clients through a network of more than 70 locations in over 20 countries. We also work with smaller, growing companies, including those looking to go public, as well as with government agencies.

Named one of the 2015 *Fortune* 100 Best Companies to Work For®, Protiviti is a wholly owned subsidiary of Robert Half (NYSE: RHI). Founded in 1948, Robert Half is a member of the S&P 500 index.

Contacts

Michael Brauneis
Managing Director
+1.312.476.6327
michael.brauneis@protiviti.com

Chris Louden
Managing Director
+1.703.350.4397
chris.louden@protiviti.com

Jeff Sanchez
Managing Director
+1.213.327.1433
jeffrey.sanchez@protiviti.com

Rocco Grillo
Managing Director
+1.212.603.8381
rocco.grillo@protiviti.com

Michael Porier
Managing Director
+1.713.314.5030
michael.porier@protiviti.com

Cal Slemp
Managing Director
+1.203.905.2926
cal.slemp@protiviti.com

Scott Laliberte
Managing Director
+1.267.256.8825
scott.laliberte@protiviti.com

Andrew Retrum
Managing Director
+1.312.476.6353
andrew.retrum@protiviti.com

David Taylor
Managing Director
+1.407.849.3916
david.taylor@protiviti.com

Mark Lippman
Managing Director
+1.571.382.7807
mark.lippman@protiviti.com

Ryan Rubin
Managing Director
+44.207.389.0436
ryan.rubin@protiviti.co.uk

Michael Walter
Managing Director
+1.404.926.4301
michael.walter@protiviti.com

[4] "Tech Giants Warn Cybersecurity Bill Could Undermine Users' Privacy," Sam Thielman, The Guardian, October 15, 2015.

protiviti®
Risk & Business Consulting.
Internal Audit.