Bloomberg BNA

Privacy and Security Law Report®

Cybersecurity

Views on Cyberthreat Information Sharing From Mark L. Krotoski of Morgan Lewis

As hacking attacks on U.S. businesses grow in intensity, the call for stronger private sector cybersecurity risk data sharing with the government has grown louder.

Bloomberg BNA Privacy & Security Law Report Senior Legal Editor Donald G. Aplin posed a series of questions to Mark L. Krotoski, a partner at Morgan Lewis & Bockius LLP in Palo Alto, Calif., about cyberthreat data sharing. Krotoski has nearly 20 years of experience as a federal prosecutor, including serving as national coordinator for the Computer Hacking and Intellectual Property Program in the Department of Justice's Criminal Division.

BLOOMBERG BNA: What are the primary concerns for companies in terms of partnering with the government to address cybersecurity issues generally and to respond to specific cyberattack threats and investigations?

Krotoski: The sharing of cyberthreat information is generally recognized as one key facet of an effective cybersecurity sharing strategy. Once information about a cyberthreat becomes known, the sharing of that information can prevent and mitigate other significant losses for others. Notwithstanding the substantial benefits that may result, presently there is a chilling effect on the sharing of cyberthreat information. Some of the primary obstacles include:

- What civil or criminal liability may result from information sharing?

- How will the government use information that is shared? For example, will the information be given to

 ISSN 1538-3423

regulators who may open an investigation on the reporting company? Will the National Security Agency use the shared information for intelligence purposes?

■ On privacy concerns, how can personal information or information identifying a particular individual be protected in sharing cyberthreat information?

■ Will shared information with the government be subject to later disclosure based on Freedom of Information Act requests?

■ What other regulatory issues are raised by information sharing? For example, when competitors in an industry share cyberthreat information, how are antitrust issues addressed?

An analogy helps explain the present challenges. Assume you live in a neighborhood where each residence has a strong security system. For some unknown reason, a few residences are burglarized without detection. If one neighbor learns how the security system is bypassed, he could share it with others. Armed with this information, the neighbors could protect themselves by addressing the security vulnerability. Law enforcement may use the information to catch the burglar. However, the neighbor may refrain from sharing the information based on fears about the consequences from the disclosure.

We need to incentive the neighbor to share the cyberthreat information without fear of the potential consequences. Until these obstacles are addressed, those who can benefit most from the cyberthreat information will not receive it.

BLOOMBERG BNA: Do you think President Barack Obama's February executive order directing the Department of Homeland Security to identify voluntary standards or guidelines for the creation industry-led information sharing and analysis organizations (ISAOs) (14 PVLR 324, 2/23/15) set the right tone for addressing those concerns and encouraging private sector participation?

The executive order is an administrative step to promote cybersecurity sharing, but it cannot be a substitute for necessary legislation that is required to accomplish the goal of meaningful information sharing.

Krotoski: The executive order is an administrative step to promote cybersecurity sharing, but it cannot be a substitute for necessary legislation that is required to accomplish the goal of meaningful information sharing. The White House recognizes the distinction since it has offered its own separate legislative proposal for information sharing that contains other substantive provisions.

While the executive order seeks to encourage voluntary information sharing, a number of unanswered questions are raised. First, it does not—and cannot—effectively address the core obstacles to information sharing. The DHS secretary is tasked to ''strongly encourage'' the development of ISAOs. However, it is questionable whether many private organizations will conclude there are strong enough incentives to participate in the absence of legislation (which would include liability and FOIA protections, among others).

Second, the order directs agencies to ensure ''appropriate protections for privacy and civil liberties'' are developed. However, the sufficiency of these protections remains to be seen.

Third, another unanswered question concerns what limitations there are on what the government will do with the information it obtains from the private sector.

Fourth, the executive order creates a new bureaucracy and new lines of authority, and it is not clear that all of them may be necessary in light of existing functions handled by others.

Further, it remains to be seen how the new structure will be implemented. Similar organizations already are used for some sectors (such as aviation, defense industrial base, financial, electricity). How will these existing information sharing entities operate with the new ISAOs? Another goal of the ISAOs is to establish best practices on information sharing. Yet, the National Institute of Standards and Technology recently published a draft guide on these issues (13 PVLR 1979, 11/17/14). In 2013, the White House directed NIST to establish a cybersecurity framework, which was issued Feb. 12, 2014 (13 PVLR 281, 2/17/14). It remains to be seen what role NIST will serve on these issues.

Ultimately, legislation will be required to provide meaningful incentives to the private sector to share cyberthreat information with sufficient privacy and liability protections and limits on the government's use of the information.

BLOOMBERG BNA: Was the executive order consistent with Obama's January legislative proposal (14 PVLR 108, 1/19/15) to grant companies liability protection when they shared cyberthreat information with the DHS National Cybersecurity and Communications Integration Center?

Krotoski: The executive order is essentially an administrative complement to the White House legislative proposal, notwithstanding some language differences. For example, both rely on the establishment of ISAOs. Both direct that an ''open and competitive process'' be used to identify a private entity to establish standards or guidelines for private information sharing. Of course, the legislation contains substantive standards that the executive order does not, such as limitations on liability and an exemption from disclosure for FOIA requests.

BLOOMBERG BNA: Does the data-sharing bill (S. 754) moved by the Senate Intelligence Committee (14 PVLR 447, 3/16/15)—that it hopes will clear Congress and be on the president's desk sometime in May (14 PVLR 597, 4/6/15)—provide any meaningful improvements or differences from Obama's proposal?

Krotoski: Bipartisan legislative momentum is building on this issue in both the Senate and House. In addition to S. 754, two other congressional committees have reported out information sharing legislation based on strong bipartisan votes.

On March 26, the House Permanent Select Committee on Intelligence reported out H.R. 1560, the Protect-

  PVLR ISSN 1538-3423

ing Cyber Networks Act, on a voice vote, to the full House (14 PVLR 546, 3/30/15).

On April 14, the House Homeland Security Committee unanimously passed H.R. 1731, the National Cybersecurity Protection Advancement Act of 2015 (*see related report*).

There are some key features in these measures that are not in the White House proposal. For example, the Senate bill would authorize ''defensive measures'' to be taken ''to protect the rights or property of the private entity'' or upon consent of''an information system of another entity.'' The Senate bill has express provisions for the sharing of information by the federal government, and the White House proposal does not. The Senate bill has an antitrust exemption provision that would allow for the exchange of cyberthreat indicators or assist in mitigating threats for cybersecurity purposes. There are some differences among the proposals on defining ''cyber threat indicator.'' Another question is which entity would receive the cyberthreat information. The White House and the House Homeland Security Committee measures would assign this function to the DHS National Cybersecurity and Communications Integration Center. The Senate bill would lead to a ''capability and process within the Department of Homeland Security,'' or ''portal,'' to receive cyberthreat information by electronic means.

It is still early in the legislative process since these measures have yet to be considered in the House or Senate. However, given the strong bipartisan, committee support, a consensus is forming on key aspects of meaningful legislation to encourage information sharing. In the past few years, information sharing legislation passed the House by a strong margin, only to die in the Senate. Now strong legislative interest is building on these issues.

BLOOMBERG BNA: Do you think the new April 1 executive order that authorized the Department of Treasury to impose sanctions on foreign individuals or entities that engage in malicious cyberattacks that threaten the economy or knowingly receive or use trade secrets stolen in such attacks (14 PVLR 578, 4/6/15) might sway private sector companies into greater information sharing with the government?

Krotoski: The order declaring a ''national emergency'' based on recent cyber espionage and malicious cyberattacks and authorizing sanctions in appropriate cases of ''malicious cyber-enabled activities''—including for ''causing a significant misappropriation'' of trade secrets—provides another tool of deterrence in appropriate cases for malicious cyberattacks. The sanctions may include the freezing of assets, denial of visas to identified hackers and barring U.S. companies from engaging in business with hackers. While it remains to be seen how frequently this new sanctions tool will be used, it provides more options to the government.

The new cyberattack sanctions executive order allows companies to conclude that by sharing cyberthreat information, the government may use a variety of tools to prosecute cybercrimals.

Significantly, the new order follows the imposition of sanctions against a country for the first time. On Jan. 2, economic sanctions against North Korea were increased based on its role in the ''destructive, coercive cyber-related actions during November and December 2014'' after the FBI announced that it had attributed to the North Korean government cyberattacks on Sony Pictures Entertainment Inc. (14 PVLR 67, 1/12/15).

Companies can conclude that by sharing cyberthreat information, the government may use a variety of tools to prosecute individuals for committing cybercrime and in appropriate cases issue sanctions. For example, where individuals cannot be extradited to the U.S., the sanctions may impose other significant penalties on those responsible for malicious cyberattacks.

BLOOMBERG BNA: Is robust pursuit of criminal prosecution of hackers by the federal government an important part of the dynamic for engendering private sector trust in a voluntary data-sharing program?

Krotoski: In our increasingly interconnected world, effectively combating cybercrime remains a key component of any national cybersecurity strategy. Law enforcement successes in combating cybercrime promote deterrence and confidence in our criminal justice system.

When private industry sees these criminal justice results, it reinforces the need to provide critical cyberthreat information to law enforcement. Private industry can contribute by providing cyberthreat information to the government with the sufficient protections we have noted

Today's cyberthreats come from many sources including state-sponsored groups engaged in cyber espionage, organized cyber syndicates, cyber terrorists and others. Cybercrime is being committed with greater sophistication than in the past. Many of the cyberattacks originate outside the U.S., making coordination with international law enforcement officials necessary.

Private industry certainly cannot address these challenges. A strong, effective ability to investigate and prosecute cybercrime remains essential. The Department of Justice Computer Hacking and Intellectual Property (CHIP) network consists of around 270 federal prosecutors around the nation. For several years, I was privileged to be a part of this network and appreciated the chance to work with many talented prosecutors around the country on interesting cases and cutting edge legal and technical issues. The CHIP network is strong and effective in addressing cybercrime issues.