Portfolio Media. Inc. | 860 Broadway, 6th Floor | New York, NY 10003 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

Cyberthreat Spawns New Era Of Public-Private Collaboration

Law360, New York (February 20, 2015, 11:02 AM ET) --

Judith Germano

On Feb. 13, 2015, President Barack Obama signed an executive order to encourage more companies and industries to engage in active information sharing, by setting up hubs for transmitting intelligence on attacks and threats. The executive order also called for common standards so government and industry can share threat information more easily. The White House also announced last week that it is creating a Cyber Threat Intelligence Integration Center, and has called for legislation to promote increased information sharing.

It is generally understood that the public and private sectors need to collaborate to address the nation's cybersecurity challenges, yet there remain significant questions regarding the circumstances, nature and scope of those relationships. Legal, strategic and pragmatic obstacles often impede effective public-private sector cooperation, which are compounded by regulatory and civil liability risks. Different government agencies have competing roles and interests, with the government serving dual roles as both partner and enforcer, influencing how companies facing cyberthreats view public authority. These domestic cybersecurity challenges are complicated further by cross-border issues, including inconsistent laws and perspectives regarding, in particular, privacy norms and restrictions, data transferability, as well as divergent political interests in combating cyberthreats.

A welter of issues involving technology, business, law and policy affect the strategic cybersecurity relationship between the government and the private sector. And many of those issues are evolving and unclear. Because cybersecurity's challenges are multifaceted, traditional modalities of interaction between government and the private sector — between regulators and regulated — do not always capture the nuanced ways in which the nature of the cybersecurity challenge has fundamentally altered these relationships.

While the problems are difficult, the answers may, in some respects, be astounding in their simplicity — solutions grounded in basic principles of organizational communication, teamwork, trust and relationship building, accountability, and foresight to prepare for and invest in mitigating risk before disaster strikes. These approaches are critically important and readily attainable, for those within industry and government who are willing to invest time, thought, and resources proactively to avoid the far greater costs of an ill-prepared cyber response strategy.

Yet, in other ways, the challenges to effective cybersecurity solutions are confounding. The technology is often complex and constantly evolving, the vulnerabilities are vast and elusive, and the laws are fragmented and unclear. Perhaps the greatest challenges emerge from the significant, sometimes competing, domestic and foreign policy consequences impacting both government and business that flow from any proposed policy or legal response. These issues emerge at the intersection of technology, risk management, business, law, and strategy; successfully navigating them requires a sophisticated understanding of each of those diverse areas.

Government and industry bring a diverse range of resources, priorities and perspectives to these issues that can sometimes compete. But, at a strategic level, they often are fundamentally aligned in their shared desire to develop effective strategic solutions to cybersecurity challenges. The key is determining how best to maximize the collective resources of business and government at that point of alignment.

Ultimately, the short answer is that no single actor (or group of actors) can figure it out alone. A strategic cybersecurity solution mandates the combined resources and coordination of government and industry, within a practical framework that balances effectiveness with efficiency, and security with privacy and innovation. To reach that solution, we first need to understand the benefits, barriers and alternatives to effective coordination, and why the nature of the problem demands new and innovative forms of collaboration. In doing so, we will come to realize that the government and private sector already are innovating in the forms of collaboration necessary to address the cybersecurity threat; next, the challenge moving forward will be to institutionalize and expand these means of working together.

An example of an innovative model of public-private cooperation to mitigate the new cybersecurity threat landscape can be found in the combined response to the crippling distributed denial of service (DDOS) attacks on American banks in 2012.[1] This was one of the largest DDOS campaigns ever launched, orchestrated by a group calling itself the Izz ad-Din al-Qassam Cyber Fighters, which disrupted service to the online banking portals of a number of major U.S. financial institutions.[2] At the peak of those DDOS attacks, U.S. banks were grappling with electronic traffic of up to 120 gigabytes per second — at least three times the volume of traffic most large bank websites were equipped to handle at the time — and banks were spending tens of millions of dollars to mitigate the problem.[3]

To address this new type of threat, the government, together with industry implemented, on a global level, a new kind of response. The U.S. government took the unprecedented step of appealing — both diplomatically and technologically — to 120 countries to help cut off the computer traffic at nodes around the world, thereby mitigating the threat. The two-pronged international appeal to counterparts overseas was made diplomatically by U.S. State Department officials and technologically by U.S. Department of Homeland Security cyber technicians.[4] While reports noted it was not a “silver bullet” to cease the attacks entirely, it did help to significantly ease the barrage of traffic that was crippling banks.[5]

At the same time, private industry also actively shared valuable threat and other information, including recommended solutions. Much of the information sharing was coordinated through the Financial Services Information Sharing and Analysis Center (FS-ISAC), which interfaces with the National Cybersecurity and Communications Integration Center.[6] This was highly effective in enabling financial institutions to thwart the 2012 DDOS attacks and to mitigate harm.[7] Since then, to further enhance its capabilities, the FS-ISAC has completed a Critical Infrastructure Notification System to allow it to send security alerts rapidly and simultaneously to multiple recipients worldwide, while authenticating users and confirming delivery.[8]

In addition to that coordination, on both a diplomatic and technological basis, to mitigate attacks, we also have seen successful coordination in identifying and pursuing attackers. For example, on May 19, 2014, the FBI announced what it described as "unprecedented cooperation" in "the largest global cyber operation to date" involving Blackshades creepware.[9] According to prosecutors, Blackshades affected hundreds of thousands of users globally, allowing users of the malicious software to secretly and remotely control victims' computers. To accomplish a takedown involving more than 90 arrests and more than 300 executed searches, the U.S. Department of Justicecoordinated with 19 cooperating countries.[10] This type of effort in the cybercrime context is particularly groundbreaking given the size of the operation, the varying level of cybercrime experience among partners in each of those countries, and the importance of operating in a swift and cross-border way to obtain significant results.

Just two weeks later, on June 2, 2014, the DOJ announced successful global operations resulting in the disruption of two massive and sophisticated cybercrime schemes related to the "Gameover Zeus" botnet and "Cryptolocker" ransomware, which also affected hundreds of thousands of computer users.[11] Through this effort, U.S. law enforcement coordinated with counterparts in more than 10 countries, and with numerous private sector industry experts in the United States.

The DOJ described Gameover Zeus, which targets banking credentials and other personal information, as "the most sophisticated botnet" that the government and its allies "ha[d] ever attempted to disrupt;" the botnet employed an estimated 500,000 to 1 million compromised computers and diverted more than $100 million dollars from victim companies' bank accounts. Cryptolocker was a pernicious and complex scheme that secretly encrypted more than 234,000 hard drives and then demanded ransom payments for giving users access to their own files and data; the DOJ cited one estimate indicating that Cryptolocker garnered more than $27 million in ransom payments in just two months.

Given the significant and evolving nature of cyberthreats, it is necessary to pool as many resources and informed perspectives as possible to address the problem comprehensively and effectively. And given the myriad extant barriers to effective cooperation, there needs to be innovation and creativity in the ways in which companies and the government do so.

To better define the collaborative landscape, and surmount the obstacles to effective cooperation on cybersecurity issues, there needs to be an ongoing dialogue among stakeholders regarding respective expectations and solutions. This dialogue should occur internally at both companies and the government, as well as between — and among — companies and the government. To ensure an effective outcome, senior executives and board members in the private sector must become acutely aware of the issues impacting their enterprise and industry, and invest time in ensuring there exist proper cybersecurity governance and strategies for effective, timely and secure information sharing internally, among private industry partners, and also with government.

—By Judith H. Germano, NYU School of Law

Judith Germano is the founding member of GermanoLawLLC and senior fellow on cybersecurity and adjunct professor of law at NYU School of Law's Center on Law and Security.

This is a modified excerpt of a white paper recently published by New York University School of Law's Center on Law and Security.

The opinions expressed are those of the author(s) and do not necessarily reflect the views of the firm, its

clients, or Portfolio Media Inc., or any of its or their respective affiliates. This article is for general information purposes and is not intended to be and should not be taken as legal advice.

[1] Nicole Perlroth, In Cyberattacks on Banks, Evidence of a New Weapon, N.Y. Times (Oct. 5, 2012, 8:30 PM), http://bits.blogs.nytimes.com/2012/10/05/in-cyberattacks-on-banks-evidence-of-a-new-weapon/.

[2] Joseph Menn, Cyber Attacks Against Banks More Severe than Most Realize, Reuters, May 18, 2013, available at http://www.reuters.com/article/2013/05/18/us-cyber-summit-banks-idUSBRE94G0ZP20130518.

[3] Ellen Nakashima, U.S. Rallied Multinational Response to 2012 Cyberattack on American Banks, Wash. Post, April 11, 2014, available at http://www.washingtonpost.com/world/national-security/us-rallied-multi-nation-response-to-2012-cyberattack-on-american-banks/2014/04/11/7c1fbb12-b45c-11e3-8cb6-284052554d74_story.html.

[4] Id.

[5] Id.

[6]See About the National Cybersecurity and Communications Integration Center, U.S. Dep't of Homeland Sec., http://www.dhs.gov/about-national-cybersecurity-communications-integration-center (discussing NCCIC's role in coordinating information sharing between the public and private sectors).

[7] Fred Donovan, FS-ISAC Threat Information Sharing Helped Thwart DDos Attacks Against US Banks, FierceITSecurity (Nov. 14, 2013), available at. http://www.fierceitsecurity.com/story/fs-isac-threat-information-sharing-helped-thwart-ddos-attacks-against-us-ba/2013-11-14.

[8] About FS-ISAC, Fin. Servs. Info. Sharing & Analysis Ctr., https://www.fsisac.com/about (last visited Aug. 26, 2014).

[9] Fran Berkman, Nearly 100 Hackers Arrested in Global Blackshades Malware Sting, The Daily Dot (May 19, 2014), http://www.dailydot.com/news/blackshades-malware-hackers-arrested-global-sting/; Aaron Katerksy, Dozens of Arrests in 'Blackshades' Hacking Around the World, ABC News (May 19, 2014), http://abcnews.go.com/ Blotter/dozens-arrests-blackshades-hacking-world/story?id=23778246.

[10] Evan Perez et al., More than 90 People Nabbed in Global Hacker Crackdown, CNN (May 19, 2014, 8:56 PM), http://www.cnn.com/2014/05/19/justice/us-global-hacker-crackdown/.

[11] Press Release, Dep't of Justice, U.S. Leads Multi-National Action Against "Gameover Zeus" Botnet and "Cryptolocker" Ransomware, Charges Botnet Administrator (June 2, 2014), available at http://www.justice.gov/usao/paw/news/2014/2014_june/2014_06_02_01.html.

All Content © 2003-2015, Portfolio Media, Inc.