Portfolio Media. Inc. | 111 West 19th Street, 5th Floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

Cybersecurity Warning May Bring Gov't, Industry Together

By **Allison Grande**

Law360 (April 24, 2018, 10:49 PM EDT) -- The U.S. and U.K. governments' recent joint warning about hacking threats from Russia offers assurance to businesses that government officials are open to working with them to combat such cyberattacks, while potentially emboldening them to push for stronger deterrence measures, attorneys say.

The U.S. Department of Homeland Security, the Federal Bureau of Investigation and the United Kingdom's National Cyber Security Centre banded together to issue the unprecedented April 16 technical alert, which warned that cyber actors supported by the Russian government are currently engaged in a "worldwide campaign" to exploit vulnerabilities in routers, firewalls and other network infrastructure devices maintained by public agencies and private companies in an effort to conduct espionage and steal intellectual property.

The warning, the first of its kind to be released jointly by U.S. and UK officials, builds on a push in recent years toward greater collaboration and information-sharing in the face of mounting cyberthreats, especially from nation-states such as Russia, North Korea and China, attorneys say. But they were quick to caution that these alerts were only an initial step, and that the growing prevalence of this type of warning is likely to prompt companies to seek even more assistance from the government, including the solidification of sanctions and international cyber norms that private companies have limited power to put into place on their own.

"Public attribution is a necessary first step in holding nation-state actors accountable for cyberattacks on the U.S. and U.S. companies, but it's not the end of the story," said David A. Simon, a Mayer Brown LLP partner and a former special counsel at the U.S. Department of Defense. "The U.S. government should do more to clarify the consequences of hacking American companies."

In recent years, the U.S. government and private companies have maintained somewhat of an "arm's-length" relationship due to federal agencies typically playing "more of an enforcement role than a collaborator or protector role" when it comes to responding to cyberattacks that impact consumers and assessing the measures businesses have taken to safeguard their systems, according to Brenda Sharton, a litigation partner and chair of Goodwin Procter LLP's privacy and cybersecurity practice.

"Especially as these threats are becoming more of a geopolitical battle, there's a growing need for cooperation between industry and government, but the government needs to create an atmosphere for industry to feel safe to do that and shift away from blaming the victim," Sharton said. "It has gotten a

little better over time, but there has to be more help for companies and more of an understanding that as long as they're following the rules, companies are victims too."

Alerts like the one issued last week help foster such an environment by demonstrating that the governments are not only taking cyberthreats seriously but also are willing to share what they've learned and treat companies as partners in mitigating these attacks.

"This type of information-sharing is one of the linchpins of a successful cybersecurity strategy," said Robert Silvers, a Paul Hastings LLP partner and former assistant secretary for cyber policy at DHS. "This is a textbook case of effective information-sharing and equipping companies in the U.S., U.K. and around the world with information about the threat and recommendations about how to guard against it."

Silvers added that while he was working at DHS, he would commonly hear companies question how they were supposed to hit back against the sizable threats posed by nation-states such as Russia or North Korea when they only have the resources of a private business.

By working together to issue the alert, the U.S. and U.K. officials are demonstrating the seriousness of the threat and their own competence in identifying and tackling it. They are also helping companies that likely wouldn't be able to detect such threats even with the best information security programs, which can now look to one alert to cover all of their bases, according to Silvers, who added that he wouldn't be surprised if these kind of joint alerts became more common.

"Companies definitely want the government to help them against actors like Russia and are looking for the government to play a role," Silvers said. "With this alert, DHS and the NCSC in the U.K. are working hard to show the value that they can provide and that they can be trusted partners."

With the information-sharing aspect getting stronger, companies are likely to push for further protections that only the government can deliver, including more indictments, sanctions and clearer rules for what won't be tolerated by other governments in cyberspace, attorneys say.

"To deter cyberactivities, the actions taken need to make threat actors think that they can be caught and will pay the price for it," Silvers added.

The U.S. government has been working in recent years to clarify and strengthen the norms of responsible nation-state behavior in cyberspace. For example, the United Nations Group of Governmental Experts released a report in 2015 that proposed numerous voluntary, nonbinding norms that nations, including the U.S. and China, have agreed to adopt, such as refraining from targeting civilian critical infrastructure and computer emergency response teams, Simon noted.

Cyber diplomacy, including the promotion of norms of responsible state behavior in cyberspace, should play a role in clarifying that malicious cyber activity against U.S. national interests and US. companies will be met with consequences, according to Simon, who also serves as an adjunct fellow for cybersecurity and international law at the Center for Strategic and International Studies.

While the executive branch could take it upon itself to implement a more explicit cyber deterrence policy, Congress could also act to help protect U.S. infrastructure and businesses threatened by state-sponsored cyber actors. A bipartisan group of House lawmakers led by Rep. Ted Yoho, R-Fla., earlier this month introduced the Cyber Deterrence and Response Act, which would require the president to not only "name and shame" malicious, state-sponsored hackers and label them "critical cyberthreats" but

also mandate that the administration impose sanctions on them for carrying out attacks against the U.S.

"The proposed legislation signals to adversaries that our Congress is also focused on the cyberthreat and that more needs to be done to defend U.S. companies and to hold perpetrators of malicious attacks responsible," Simon said.

Companies are likely to view such actions favorably and may even push for their formalization, especially in light of their growing appetite for taking an aggressive stance toward these threats, attorneys say.

Just last week, more than 30 technology companies and cybersecurity firms, led by Microsoft and Facebook, pledged not to help any government launch cyberattacks on "innocent citizens" around the world, as part of a sweeping new agreement over conduct in cyberspace. The accord also calls for companies to work together to protect all of their users and customers "irrespective of their technical acumen, culture or location, or the motives of the attacker, whether criminal or geopolitical."

But the limits of how far private companies can go to cut down nation-state threats are obvious, meaning they'll need the government to fill those gaps and make similar pledges to be tough on those who threaten U.S. infrastructure and systems, attorneys noted.

"Given that U.S. law, such as the Computer Fraud and Abuse Act, prohibits companies from hacking back, the U.S. government has a critical role to play in deterring state-sponsored cyber actors for attacking U.S. companies and for holding them accountable," Simon said.

While these protections appear to be attainable, they may take time, with attorneys noting that the government didn't begin its deterrence tactic of naming and shaming suspected nation-state hackers until it attributed the destructive 2014 cyberattack on Sony Pictures Entertainment to North Korea.

Now, that practice is far more common. During the past year, the U.S. government has blamed Russia for the NotPetya cyberattack that paralyzed part of Ukraine's infrastructure and wreaked havoc on computers worldwide, including at DLA Piper; for a targeted attack on critical infrastructure providers; and for interfering with the 2016 presidential election. The government followed these announcements up by imposing new sanctions in early April on dozens of Russian officials and entities for, in part, "cyber actions" taken against the U.S. and other countries.

While companies await more robust consequences such as enhanced sanctions to be put in place, they would be wise to heed the advice in alerts such as the one issued last week, which highlighted a common vulnerability in routers and other internet infrastructure that hackers are regularly trying to exploit, attorneys say.

"As with so much in cybersecurity, the news that's surprising and shocking isn't what could be done, but rather that someone is actually doing it," Silvers said, adding that the threat of Russian hackers compromising routers and other networking gear is "incredibly serious" because it would allow "unprecedented visibility" into information flows and the ability to manipulate information on a large scale.

According to the alert, companies should take steps that attorneys characterize as primarily widely known and accepted practices to mitigate these threats, including blocking unencrypted management

protocols from entering an organization from the internet, refusing to allow access from the internet to the management interface of any network device, disabling legacy protocols and replacing default passwords with a "strong password policy."

"The only thing truly surprising here is that anyone would be surprised that the Russians or other advanced cyberthreat nations would be targeting routers on a large scale," said Pillsbury Winthrop Shaw Pittman LLP partner Brian Finch. "It's a reminder that every connected device is a potential espionage device, so companies handling sensitive materials or information always need to be cognizant of the need to use more secure communications channels and devices ... [and they] cannot simply go purchase devices or components from the lowest-cost bidders anymore if they truly care about security."

--Editing by Pamela Wilkinson and Alanna Weissman.
