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

Move To Pin DNC Hack On Russia Needs Strong Follow-Up

By **Allison Grande**

Law360, New York (October 12, 2016, 7:05 PM EDT) -- The U.S. government's recent decision to publicly blame Russia for hacking into the Democratic National Committee indicates that federal officials are taking these cyberthreats seriously, but the long-term efficacy of this name-and-shame tactic will likely turn on what federal officials choose to do next.

In a joint statement issued Friday, U.S. intelligence officials announced that they were "confident" that the Russian government had directed a cyberattack of the DNC that came to light in July and led to the disclosure of tens of thousands of internal emails on WikiLeaks and elsewhere.

Officials said that the "scope and sensitivity" of the hack led them to believe that "only Russia's senior-most officials" could have authorized these activities and that the attack was carried out in order to "interfere with the U.S. election process."

"In the grand scheme of things, given that the U.S. does not make many public attributions of this nature and has been reluctant to do so in this case for months, this move reflects the level of seriousness with which the government takes this issue," Mayer Brown LLP partner Marcus Christian said. "For a nation that prides itself on democracy, it would have been hard for the government to sit idly by and watch a foreign power commit acts that seem to undermine that very democracy."

Both businesses and the government are increasingly being targeted by sophisticated nation-state hacks. They're especially tricky to combat given that these actors are generally highly motivated and exceedingly sophisticated in the tactics they use to both break into systems and to remain there undetected, experts say.

"You can easily take a $10 billion company offline from thousands of miles away with a few keystrokes," said Andrew Ostashen, co-founder and principal security consultant at Vulsec LLC.

Many major U.S. companies have found themselves caught up in nation-state hacks in recent years. Most recently, Yahoo claimed that the newly disclosed 2014 attack that compromised data tied to at least 500 million user accounts was carried out by "a state-sponsored actor." And in December 2014, the FBI squarely placed the blame on North Korea for a massive cyberattack at Sony Pictures Entertainment Inc. that compromised the personal and health data of thousands of current and former employees, as well as vast quantities of sensitive proprietary information.

Many businesses have responded by tightening up their security and detection protocols and moving to

share more data about cyberthreats both with one another and with the government. But it's the government's response to such incidents that's particularly vital because it has tools — such as the ability to wield sanctions, bring public prosecutions and launch strategic countermeasures that are carefully considered — that the private sector lacks.

"I'm sure that the government's announcement about Russia was strategic and wasn't done without a tremendous amount of thought given to it," said Brenda Sharton, a Goodwin litigation partner and chair of its privacy and cybersecurity practice. "When a nation is speaking and it says that it knows it was a particular actor, there are a whole host of different political and economic implications that would need to be factored into the determination to name that actor publicly."

The U.S. likely decided to take the rare step of publicly naming Russia as the culprit for the DNC hack in order to provide some level of deterrence to future attacks, experts said.

"By letting them know that the government was able to figure out the origin of the cyberattack, that perhaps gives the attackers pause and provides some deterrence, depending on the reaction of the country," Sharton said.

But what the U.S. elects to do next will almost certainly be the primary factor in assessing whether the tool has the desired effect of making sure that nation-state actors know that hacking the U.S. is risky, according to experts.

"Now that we have the attribution, it will be important to watch to see whether a robust package of sanctions will follow," Christian said. "Because if it's only an announcement, that might in the long run have a negative impact, by showing that it was just idle words with nothing to back it up."

White House spokesman Josh Earnest told reporters on Air Force One on Tuesday that President Barack Obama would consider a "range of responses" to Russia's hacking of the DNC and that it was "certainly possible" that Obama would choose options that would not be publicly disclosed.

Pressure has been mounting on the White House to back up its talk with action, most notably from lawmakers who want to see something done to punish the accused party.

On Friday, Republican Sen. Cory Gardner from Colorado, who chairs the Senate Foreign Relations subcommittee on East Asia, the Pacific and International Cybersecurity Policy, vowed to introduce legislation that sanctions the Russian cybercriminals. The proposal — which is similar to one that Gardner made in a separate move to sanction North Korea in the wake of the Sony attack — would mandate that the Obama administration investigate the individuals who have engaged in "significant activities undermining cybersecurity" and "aggressively pursue sanctions" when appropriate, according to the lawmaker.

"Russia’s interference with American democracy is a direct threat to our political process, and it may only be the tip of the iceberg," Gardner said. "It is imperative that Russia’s behavior is met with strength in the form of aggressive sanctions to show the world that its cybercrimes will not be tolerated.”

The White House did answer the call to hit back against North Korea in the wake of the Sony hack. In January 2015, Obama imposed economic sanctions against several North Korean government agencies and senior officials in retaliation for the country’s alleged role in the breach, which was found to be payback for Sony's distribution of "The Interview," a movie in which North Korea's leader Kim Jong-un is

assassinated.

The president followed up on that move by handing down an executive order in April 2015 that established a new sanctions regime that enabled the administration to level harsh penalties against individuals overseas who carry out “malicious” cyberattacks that threaten crucial national security and economic interests.

While Obama renewed that authority earlier this year, saying that the nation is still facing a state of emergency regarding cyberintrusions, no person or company has been sanctioned for such an intrusion. But that executive order was widely seen as a way to send a clear political message to nations such as North Korea and China, which is regarded as the origin of some of the most egregious cybersecurity intrusions.

U.S. government officials have taken a slightly different tack in going after China, electing in 2014 to charge five members of the state-backed People's Liberation Army with conspiring to hack into the computers of Alcoa Inc., U.S. Steel Corp. and four other entities to steal sensitive information that would be "useful to their competitors" in China, including state-sponsored enterprises.

Officials again chose to take the prosecution route earlier this year in charging seven individuals who purportedly have ties to the Iranian government with orchestrating cyberattacks against banks, stock exchanges and a New York dam.

While prosecutors have not been able to track down and arrest the hackers in either case, experts have said that both actions could still have a deterrent effect by demonstrating the U.S. government's willingness to take aggressive steps against state-sponsored hackers and discouraging individuals from taking actions that could land them in hot water criminally.

The public denouncement of Russia by itself is similarly seen as being a strong move, albeit a largely symbolic one at the moment.

"While publicly denouncing a nation-state is likely meant to send a message to the hackers that the government is on your tracks and to cut out what you're doing, that action on its own just seems like a propaganda tactic, in that the U.S. is just publicly denouncing someone that they don't trust and know is doing shady stuff on the internet," Ostashen said. "It's just finger-pointing at this point."

But taking additional actions such as imposing hefty sanctions or bringing criminal charges could help lend more weight to such public namings, although any such follow-ups will need to be weighed carefully by U.S. officials against the risks of levying such robust penalties on a nation as powerful and adverse to U.S. interests as Russia, experts said.

"There's no silver bullet for all of this, which is one of the most unsatisfying things when you talk about cybersecurity," Christian said. "The U.S. government seems to be taking a more aggressive stance and has equipped itself with more tools for dealing with foreign powers that want to hack into our systems, but it really remains to be seen what will come next."

Both the public and private sector would also benefit from most aggressive steps from bodies like the United Nations, which has long been pushed to regulate nation-state hacking and to classify cyberwar as a form of theft that is met with serious repercussions, experts say.

"Right now, it's the Wild West and anything goes," Ostashen said. "There are regulations that can put private individuals in jail if they hack an organization without authorization, but there's nothing coming down nation-state to nation-state that formally restricts these activities."

Besides being important from a deterrence standpoint, the ability of the U.S. government to mount a significant response with serious and long-lasting consequences is also vital for sending a strong message to the private sector that cybercrime should be of the highest importance to them as well, attorneys say.

"To the extent that businesses are not treating cybersecurity with the same level of seriousness, the government's move raises the profile of the issue and is saying that this is something that business needs to be paying attention to, investing in and focusing on more heavily," Christian said. "In the cyber world, every neighborhood is a bad neighborhood, and both the government and private organizations have a role to play."

--Editing by Mark Lebetkin and Patricia K. Cole.
