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

US Must Use 'Full Toolkit' To Fight Cybercrime: Ex-DOJ Chief

By **Ben Kochman**

John Carlin

Law360 (November 15, 2018, 10:08 PM EST) -- The Kremlin will keep mounting cyberattacks aimed squarely at America's democracy as long as such efforts are worth the risk, says the man who once led the U.S. Department of Justice's national security efforts.

"We're doing better than we have done in the past, but not enough, because we're not succeeding in changing the calculus," said John P. Carlin, who ran the DOJ's National Security Division from April 2014 to October 2016 and then went into private practice at Morrison & Foerster LLP. "Russia still views, for instance, what it did in 2016 to undermine confidence in our democracy as a success."

Despite public rebukes and federal indictments, cybercriminals in places like Russia, China, North Korea and Iran continue to attack U.S. companies and infrastructure, Carlin writes in his new book, "Dawn of the Code War: America's Battle Against Russia, China, and the Rising Global Cyber Threat."

Changing that equation will require a deterrence campaign that includes sanctions, more indictments and even some offensive cyberattacks mounted by the U.S., Carlin writes in the book, which was co-authored with journalist Garrett Graff.

The book goes behind the scenes into how law enforcement responded to headline-grabbing data episodes like the 2014 hack into Sony Pictures and the 2015 theft of 21.5 million personal records stored in the U.S. Office of Personnel Management by operatives in China.

Carlin, who now chairs MoFo's global risk and crisis management practice group, shared his thoughts with Law360 on a range of topics, including what he expects from the probe into Russian interference in U.S. elections led by Special Counsel Robert Mueller, whom Carlin served as chief of staff when Mueller was FBI director. This interview has been edited for length and clarity.

What measures should the U.S. take to deter cyberattacks from enemies?

We moved faster than any other country in the world at moving information from books and papers to digital and connecting it to the internet, and we continue to innovate and rely on that technology. But just because [foreign nation-states] hit us where we're vulnerable, that doesn't mean we should hit

them back in the same sphere. A cyberattack does not equal cyber retaliation. What we should do instead is calculate where are they vulnerable and where are we strong.

The success of our program is raising the cost sufficiently to deter this type of activity. One tool that we have to do that is the credibility and reach of our criminal justice system. A second tool is the world's reliance on our financial system, and therefore sanctions. A third is the reliance of companies on our technology, so we can use Commerce Department authorities to designate entities who are contrary to the national security interests of the United States.

We can apply diplomatic pressure by working with international partners to do all of the above, and we can also take action against embassies. [Offensive cyberattack] operations from our Cyber Command can be one of those tools, but we should put together a package using that full toolkit that raises the cost proportionally to change that behavior.

What steps should the government, private industry and consumers take to promote better cybersecurity practices?

There are three areas to tackle. One is, as we move toward the internet of things, whether it's through voluntary standards or government regulation or law or some combination thereof, we need to incentivize security by design on the front end, so that we're meeting minimum requirements and so that there's more transparency for customers about what they're buying.

We're also facing a critical education gap. I think every student as part of their curriculum should learn about online safety and risk as part of their primary education. And we need to provide the funding and curriculum to meet the critical skills gap when it comes to cybersecurity jobs.

And at the high end for those who program, we need to make sure that it's part of the curriculum, so that anyone who programs is at least getting Cybersecurity 101. That was not true, and I think it's still not true even at some of our most elite universities. You can go all the way through and never really learn about cybersecurity.

As an ex-government official, what advice do you give firms deciding when to tell authorities about a data breach?

Right now, we have a confusing system of carrots and sticks, and so often the decision as to when to inform law enforcement focuses on downside risk. There's uncertainty: "What might happen with regulators or how this might affect a suit later? Will we lose control of the process?"

Those are legitimate questions, but many companies, and this became clear when I was talking to them, didn't know some of the worst-case scenarios that we have seen. We're not thinking through the downside of not telling law enforcement if this takes a turn for the worse in an era where the first question if something becomes public is, "When did you tell law enforcement?"

A cyberattack does not equal cyber retaliation. What we should do instead is calculate where are they vulnerable and where are we strong.

JOHN CARLIN

When presented with that, and understanding what the full risks are, then companies can make good risk decisions.

Should the government be doing more to incentivize private companies to cooperate?

Are we there right now with the carrots and sticks? I don't think so. The government's come a long way, in particular the FBI and Justice Department. There's been a real change in my 20 or so years working there to better accommodate the interest of the victim, of the company, but there are still so many overlapping state and federal regulations that provide competing incentives.

Some are very punitive and incentivize you not to tell or to wait to tell, and others are saying, "Come and tell us." So it's an area where it still works to rationalize the different regimes and make them consistent. ... It's helpful being here in private counsel to be able to walk people through who to tell in government and how to tell them. But it has also become really clear that if you don't have someone expert in that area, it's not that easy to navigate.

How do the see the Russian interference probe being led by your ex-boss Robert Mueller playing out?

You know, if I wasn't out of time, I would tell you exactly how it is going to end! [*Laughs*] The one thing I say, and it sounds a little "Boy Scouts," is that I've had the privilege of working with a lot of very talented people over the years, but there is no one more dedicated to doing his mission, following the facts wherever they might lead and applying the law than Bob Mueller.

That's been true throughout his career as a prosecutor, as the leader of the Justice Department's Criminal Division and the FBI, and it's true now. So the one thing I know is that wherever it ends up, it will have been a by-the-book professional investigation.

--Editing by Jill Coffey and Alanna Weissman.