LAW360

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 Pros On Edge As Biden Warns Of Russia Threat

By **Ben Kochman**

*Law360 (March 31, 2022, 10:05 PM EDT)* -- An ominous White House warning that Russia may soon launch cyberattacks on U.S. critical infrastructure and the release of an indictment detailing the Kremlin's alleged past hacking schemes have cybersecurity advisers urging companies to shore up their defenses.

President Joe Biden's March 21 statement that his office has "evolving intelligence that the Russian government is exploring options for potential cyberattacks" in response to international sanctions is part of a broader strategy shift to speak more openly about digital threats than previous administrations have, cybersecurity attorneys say.

To hammer home its point about the dangers of Russian nation-state-backed cybercrime, the U.S. Department of Justice also unsealed an August 2021 indictment days after Biden's statement, charging four Russian government employees with orchestrating sprawling hacking schemes targeting the global energy sector in 135 different countries between 2012 and 2017.

The suspected Russian operatives allegedly targeted oil and gas firms, nuclear power plants, and utility and power transmission companies in attacks that could have given Russia the chance to cause "potentially catastrophic" physical damage, prosecutors said.

Since Russia's invasion of Ukraine, which began in late February, a cyberattack on U.S critical infrastructure at the level of several high-profile 2021 intrusions has yet to emerge. Criminal ransomware gangs breached networks belonging to a key fuel pipeline and a meat processing giant in May 2021 alone.

But companies in the energy, financial, health care, communications and other critical sectors should still heed the government's advice to patch known software flaws and make sure they have a game plan in place for dealing with attempted attacks, cybersecurity experts say.

"The U.S. government does not cry wolf," said Brandon Van Grack, a Morrison & Foerster LLP partner and former senior DOJ official. "They would only be doing this if they had real, actionable intelligence and concern that this malicious cyberactivity is about to happen."

Malicious cyber actors linked to the Russian government have taken preliminary steps toward a potential attack on U.S.-based entities, including by scanning target networks and hunting for new or existing software vulnerabilities, White House deputy national security adviser Anne Neuberger said at a

March 21 press briefing.

The Cybersecurity and Infrastructure Security Agency also released technical details about the tactics used by Russian actors in past attacks.

Any decision by the U.S. government to release information on the nuts and bolts of how Russia or other nation-state-backed actors are carrying out cyberattacks is part of a calculated balancing act between helping targets avoid risk and potentially tipping off the attackers to how much U.S. investigators know about their operations.

The intrusions highlighted by CISA are all from earlier attacks, the agency's Director Jen Easterly said in a statement.

Yet the "associated tactics, techniques, procedures and mitigation steps are still highly relevant in the current threat environment," Easterly added.

CISA and U.S. law enforcement agencies have been making an effort recently to share information about cyberthreats with potential targets, both publicly and in classified briefings, while urging companies to report data breaches even when they may not be mandated by law to do so, administration officials say.

"The more companies are aware of a significant vulnerability in a commonly used piece of software, the more companies can take action to protect themselves," said Jena Valdetero, co-chair of the U.S. data privacy and cybersecurity practice at Greenberg Traurig LLP. "Companies need that type of granular information."

Exposing how groups carried out certain attacks in the past could also force attackers to "be more creative in their approach in the future," Valdetero said. Still, attackers have been up to that task, she said.

"These cybercrime groups are nimble and they're really adept at reinventing themselves," Valdetero added.

The U.S. government's advice for potential targets of Russian cyberattacks includes scanning their networks for any known security vulnerabilities that intruders could use to access their systems. U.S. officials have been seeing a "troubling" amount of compromises of U.S. businesses that involve known hacking risks, Neuberger told reporters in a recent press briefing.

The administration has also shared on CISA's website a list of best practices companies can follow, including requiring third-party software vendors to follow heightened security guidelines and using two-factor authentication to gain access to company systems.

The warning about Russian activity in cyberspace is just the latest move by the Biden administration to proactively notify the public about cybercrime risks even before a major incident unfolds.

In February, for instance, the White House cautioned businesses about a flaw in Log4j, a common piece of software used to record activities within the computer systems of millions of consumer-facing devices. The vulnerability allows an attacker to remotely take over a victim's systems and put in place malicious code that could be activated later, leaving open the possibility that an intrusion could be uncovered months or years after the initial attack, federal officials said.

The government's push to bring more attention to cybersecurity risks comes as the pace of cybercrime continues to rise, with attackers taking advantage of security gaps stemming from employees working from home amid the COVID-19 pandemic.

"The federal government making the American people more aware of cybersecurity risks is good leadership," said Cyrus Vance Jr., global head of the cybersecurity practice at Baker McKenzie. "And good leadership is what's required in order to appropriately deal with the surge in cyberattacks that we've seen over the past few years."

--Additional reporting by Hailey Konnath. Editing by Alanna Weissman and Lakshna Mehta.

---