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

White House Strategy Prompts Debate Over 'Secure' Software

By **Ben Kochman**

Law360 (April 7, 2023, 8:33 PM EDT) -- The Biden administration's plan to hold developers liable for selling hackable software would provide a key financial incentive to build secure products, but could also lead to a cornucopia of litigation, cybersecurity attorneys say.

White House officials said last month that they plan to work with Congress to develop legislation establishing cybersecurity liability for software providers who sell their products to organizations that later suffer a data breach. Such a law would also provide a safe harbor for companies that "securely develop and maintain" their products, following guidelines established by organizations like the U.S. Department of Commerce's National Institute of Standards and Technology.

The proposed liability shift outlined in Biden's national cybersecurity strategy is a response to a series of high-profile cybersecurity episodes that have stemmed from hacks targeting software vendors. Such attacks have allowed the intruders to use their initial target as a launching-off point to find their way into networks belonging to dozens or even hundreds of the vendor's clients.

The plan reflects federal officials' view that software developers have not shouldered adequate responsibility for releasing products bearing cybersecurity flaws. Jen Easterly, director of the Cybersecurity and Infrastructure Security Agency, argued in a February speech that companies or individual consumers should expect tech providers to provide secure products in the same way that motorists expect their cars to have seatbelts and airbags.

Cybersecurity attorneys are paying close attention moving forward to how the administration defines the cybersecurity equivalent of a digital "seatbelt" or other security measures that could grant providers a highly valuable prize — potential immunity from litigation.

"This is a real opportunity for liability not to be seen as a detriment, but to be seen as an opportunity for companies to invest," said Evan Wolff, co-chair of the privacy and cyber group at Crowell & Moring LLP. "The concept of a safe harbor will be transformative to how companies manage their development cycle."

Courts across the country have for years grappled with questions over who can be held liable in the wake of cyberattacks, and software providers whose products have had security flaws used to carry out hacks on their customers have faced lawsuits. Evidence released by U.S. authorities that foreign governments like Russia and China have sponsored intrusions on U.S. organizations has meanwhile complicated the question of what it means for a company to take "reasonable" steps to prevent an

attack or mitigate damage.

Such principles that could lead to a form of safe harbor for software providers could include providing evidence of having "secure coding practices" and transparent processes for security researchers to disclose cybersecurity flaws they've discovered, Easterly said during the February remarks at Carnegie Mellon University. Other details would need to be hashed out in the coming months, but it's clear that officials feel that the existing status quo — which places the onus on customers to regularly root through their systems to update software known to be flawed — is not working.

"The proposed liability shift reflects a view by the Biden administration that market forces alone haven't done enough to drive companies to build secure software, and that too many attacks happen because of regularly occurring vulnerabilities," said Alex Iftimie, a privacy and data security partner at Morrison Foerster LLP.

Administration officials have not explained how exactly their proposed liability shift would be enforced. Given that there is no one federal regulator that oversees the software industry, it's not clear whether legislation would grant an agency like the Federal Trade Commission new powers, or carry with it a private right of action.

If businesses are given runway to sue their software providers in the wake of a data breach, they would likely do so aggressively, said Erez Liebermann, a member of the data strategy and security group at Debevoise & Plimpton LLP.

Yet, lawmakers would need to first navigate the thorny issue of how to define "secure" software, given that skilled hacking groups have shown an ability to infiltrate even high-level defenses, he added.

"We all accept that the idea that perfect cybersecurity is a myth," Liebermann told Law360. "Even top-of-the-line security and software development will have vulnerabilities."

Adding a new avenue for consumers or businesses to bring lawsuits against software providers may be also a challenge in Congress, given that disagreements about a private right of action have helped stall efforts to pass a national data privacy law through the chamber.

In the short term, the administration may be better served to drive best practices in the software sector by having government agencies only accept contracts with vendors that meet higher standards, Iftimie said.

"My sense is that the government will more easily drive the changes it is seeing through changes in its procurement process, rather than by threatening companies with liability for releasing buggy products," he added.

--Editing by Emily Kokoll and Alanna Weissman.
