JENNER & BLOCK

Client Alert: White House Doubles Down on Private Sector Outreach for Cybersecurity Push

Publications

June 8, 2021
By: David Bitkower, Aaron R. Cooper, Tali R. Leinwand, Shoba Pillay, David Robbins

The White House sent an open letter last week to "corporate executives and business leaders" urging their companies to take "immediate steps" toward better protecting themselves against ransomware attacks.[1] Although the White House cannot generally dictate the actions that private companies take, the Biden administration has emphasized that "[b]usiness leaders have a responsibility to strengthen their cyber defenses to protect the American public and . . . economy."[2] To that end, the letter referenced the five "best practices" set forth in the recently issued Executive Order on Cybersecurity, including (1) multifactor authentication; (2) endpoint detection; (3) endpoint response; (4) encryption; and (5) a skilled and empowered security team. The letter also outlined five basic but impactful security practices that the White House recommended companies implement:

- ***Back-up Data.*** Back-up data, system images, and configurations, regularly test them, and keep the backups offline. If network data is encrypted with ransomware, the organization may still be able to restore its systems.
- ***Update Systems.*** Promptly update and patch systems, including applications and firmware.
- ***Test Plans.*** Test incident response plans to help identify gaps and understand how long business operations can be sustained without access to certain systems.
- ***Conduct Independent Checks.*** Check the security team's work and ability to defend against a sophisticated attack, thereby increasing the likelihood that back doors or other loopholes can be addressed.
- ***Segment networks.*** Separate corporate business functions from manufacturing and production operations, and limit internet access to operational networks.[3]

The letter, which was authored by Anne Neuberger, Deputy National Security Advisor for Cyber and Emerging Technology, was sent in light of a reported uptick in attacks involving ransomware

(software that seizes control of a computer until the victim pays a fee), most recently an attack that reportedly closed off beef and pork production from one of the country's leading food suppliers.[4]

The letter also reflects the Biden administration's growing emphasis on the need to improve the government's cybersecurity defenses, both within and across various agencies. Yesterday, in a press conference regarding the ransomware attack on Colonial Pipeline, Deputy Attorney General Lisa Monaco emphasized that companies should take preemptive action against ransomware attacks, urging them to "pay attention now" and "invest resources now" because "[f]ailure to do so could be the difference between being secure now – or a victim later."[5] The press conference came just a few days after Deputy Attorney General Monaco issued an internal memorandum directing US prosecutors to report all ransomware investigations that they may be working on, stressing the need for better coordination within the Department.[6] Two weeks ago, the Department of Homeland Security's Transportation Security Administration announced a security directive requiring pipelines to report confirmed and potential cyber incidents and review current cybersecurity practices.[7] And last month, the White House issued the Executive Order imposing a variety of requirements on federal agencies and government contractors that are aimed at improving the government's cybersecurity defenses.

As companies seek to evaluate cybersecurity and expand their protections, it is important to consider the following legal issues alongside business and technical concerns:

- ***Importance of a Multi-Functional Team.*** Cybersecurity and information protection are broad efforts encompassing many different skills within a company. Legal counsel should be included in the team to advise about the application of relevant laws, regulations, and policies, and to prepare for potential litigation and enforcement actions.

- ***Importance of Legal Privilege.*** Companies should consider how to maximize the application of legal privilege to internal factfinding efforts that are designed to address potential legal exposure from cybersecurity and data protection rules.

Outside counsel can help bolster in-house teams and provide broad industry perspective on common issues in these reviews. Jenner & Block lawyers stand ready to assist.

Footnotes

[1] Letter from Deputy National Security Advisor for Cyber and Emerging Technology Anne Neuberger to Corporate Executives and Business Leaders (June 3, 2021).

[2] Press Briefing by Press Secretary Jen Psaki (June 3, 2021); see also Tucker Higgins, CEOs Need to Prepare Now for Exponential Increase in Ransomware Attacks, Top DOJ Official Says, CNBC (June 4, 2021).

[3] Letter from Deputy National Security Advisor for Cyber and Emerging Technology Anne Neuberger to Corporate Executives and Business Leaders (June 3, 2021).

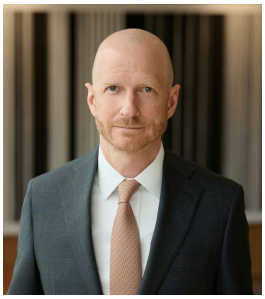
[4] David E. Sanger and Nicole Perlroth, White House Warns Companies to Act Now on Ransomware Defenses, N.Y. Times (June 3, 2021).

[5] Office of Public Affairs, Department of Justice, DAG Monaco Delivers Remarks at Press Conference on Darkside Attack on Colonial Pipeline (June 7, 2021).

[6] Deputy Attorney General Lisa Monaco, Memorandum for all Federal Prosecutors on Guidance Regarding Investigations and Cases Related to Ransomware and Digital Extortion (June 3, 2021).

[7] Press Release, DHS Announces New Cybersecurity Requirements for Critical Pipeline Owners and Operators, Department of Homeland Security (May 27, 2021).

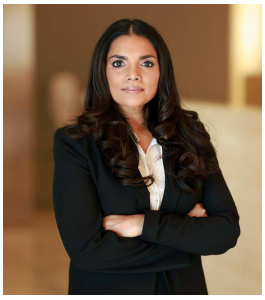
Related Attorneys



David Bitkower
Partner
dbitkower@jenner.com
+1 202 639 6048

Aaron R. Cooper
Partner
acooper@jenner.com
+1 202 637 6333

Tali R. Leinwand
Partner
tleinwand@jenner.com
+1 212 891 1697



Shoba Pillay
Partner
spillay@jenner.com
+1 312 923 2605

David Robbins
Partner
drobbins@jenner.com
+1 202 639 6040

Related Capabilities

Data Privacy and Cybersecurity

Related Locations

Chicago

New York

Washington, DC

Stay Informed →