Litigation & Arbitration Group

Client Alert

Milbank

White House Outlines "Critical Responsibility" of Private Sector in Protecting Itself from Ransomware Attacks

June 9, 2021

Contact

Adam Fee, Partner
+1 212.530.5101
afee@milbank.com

Chris Gaspar, Partner
+1 212.530.5019
cgaspar@milbank.com

Joel Harrison, Partner
+44 20.7615.3051
jharrison@milbank.com

Charles Evans, Partner
+44 20.7615.3090
cevans@milbank.com

Tawfiq Rangwala, Partner
+1 212.530.5587
trangwala@milbank.com

On June 3, 2021, the White House took the bold step of expressly warning companies to urgently take specific steps to protect themselves from ransomware attacks. High-profile ransomware attacks in the U.S. have escalated recently, crippling infrastructure (the Colonial Pipeline) and disrupting food supply (nine JBS Foods USA's beef plants). The White House's call to action represents an important step by the U.S. government both to raise awareness of threat actors *and* to recommend actions companies can take to protect themselves in this environment.

Although not explicitly threatened in the White House's message, it is safe to assume that federal and state regulators in the U.S. and in other jurisdictions may consider whether companies heeded this warning in assessing the adequacy of corporate cybersecurity measures. For example, recent actions by the New York Department of Financial Services against financial institutions under New York's Cybersecurity Requirements for Financial Services Companies, or by the California Attorney General against the maker of a women's healthcare application, signal increased scrutiny of corporate cybersecurity systems and controls, even where no breach has occurred. See related client alerts:

- "Regulator Brings First-Ever Enforcement Action under New York's Financial Services Cybersecurity Regulation" (July 29, 2020)

- "Cybersecurity, Protecting the Grid & Digital Infrastructure: Executive Order to Counter Threats to U.S. Bulk-Power System" (May 4, 2020)

The recent spate of ransomware attacks means that law enforcement and regulators will likely have less tolerance of entities that have failed to proactively guard against such attacks or have plans in place for how to handle such attacks when they occur.

The Open Letter and Its Recommended "Immediate Steps"

Issued by the National Security Council (Anne Neuberger, Deputy National Security Advisor for Cyber and Emerging Technology), the open letter to "Corporate Executives and Business Leaders" outlines the following steps organizations can take to protect themselves:

- Implement multifactor authentication, endpoint detection and response, encryption, and “a skilled, empowered security team”

- Ensure backups of data, system images, and configurations exist, are kept *off network,* and are tested regularly

- Update and patch systems promptly, including operating systems, applications, appliances, firmware, and devices using a centralize patch-management system

- Test incident-response plans by running through real-life scenarios that determine whether a business can continue operating without access to certain systems and, if so, for how long

- Check security systems using a third-party tester who can help identify any unlocked doors

- Segment networks to avoid disruption of operations. Corporate business functions should be separated from manufacturing/production operations, for example. Internet access between operational networks should be filtered and limited

- Once links between networks are understood, workarounds or manual controls should be developed to ensure industrial control systems (ICS) networks can be isolated and continue operating in the event of an attack

The open letter follows the President’s May 12, 2021, Executive Order containing a multi-step plan to modernize the government’s cybersecurity defenses and protect federal networks.

Additional Resources

Milbank attorneys have extensive experience of counselling global companies and financial institutions facing ransomware attacks. Our work has included advising on the initial incident response, engagement with law enforcement and other agencies, requirements of data privacy legislation and other laws and regulations, and internal investigations, as well as on civil liability and regulatory proceedings that have followed. We have also counselled clients on reviewing and hardening their policies, procedures and systems for dealing with ransomware and other cybersecurity threats. If you have questions about the White House’s open letter, or have experienced a ransomware attack, or if you are concerned about the risks posed by ransomware, Milbank’s cybersecurity team can offer solutions to help guide your enterprise.

Open Letter: “What We Urge You To Do To Protect Against The Threat of Ransomware”

FACT SHEET: President Signs Executive Order Charting New Course to Improve the Nation’s Cybersecurity and Protect Federal Government Networks

Contacts

London | 10 Gresham Street, London EC2V 7JD

Charles Evans	cevans@milbank.com	+44 20.7615.3090
Joel Harrison	jharrison@milbank.com	+44 20.7615.3051

New York | 55 Hudson Yards, New York, NY 10001-2163

Adam Fee	afee@milbank.com	+1 212.530.5101
Christopher J. Gaspar	cgaspar@milbank.com	+1 212.530.5019
Tawfiq S. Rangwala	trangwala@milbank.com	+1 212.530.5587

Litigation & Arbitration Group

Please feel free to discuss any aspects of this Client Alert with your regular Milbank contacts or any member of our Litigation & Arbitration Group.