Freshfields Bruckhaus Deringer

Draft Cyber Breach Bill Needs Stronger Federal Involvement

Authored by: Brock Dahl
October 19, 2021

The following article was published by Bloomberg Law on October 19, 2021. Click here to view. Republished with permission.

Congress needs to require more than just better and faster reporting in federal cyber breach legislation working its way through the Senate, says Brock Dahl, counsel at Freshfields Bruckhaus Deringer. He suggests a range of federal government obligations be added to help combat international cyber threats and breaches.

Imagine a world where a foreign army stormed the California coast-line, smashed into technology companies around Silicon Valley, stole every computer and information storage device, and then returned home without so much as a hand slap.

Or, imagine armies of foreign organized crime syndicates, operating with pseudo-state cover, flying into cities across the eastern seaboard, walking into companies with guns drawn to the heads of corporate executives and IT staff, shutting down all operations, and forcing the executives to cough up millions of dollars before the criminals returned home.

Stated in such physical terms, the scenario seems shocking; why is it any less appalling that the cyber equivalent happens daily in cities across the U.S.?

Corporate America, large and small, the lifeblood and driving growth of the American economic miracle, is being savaged by foreign antagonists. The Senate Homeland Security and Governmental Affairs Committee has proposed to address the problem through a draft bill requiring "critical infrastructure entities" to report cyber breaches to the Department of Homeland Security within 72 hours, and requiring all entities with more than 50 employees to report when they have paid a ransom. (Those who don't face subpoenas and sanctions.)

This is the latest in a series of proposals in Washington intended to address the scourge of cyber hacks, many of which involve ransomware demands, primarily through means of information sharing with the federal government.

What Will Sharing Information Accomplish?

The policy assumption seems to be that such sharing will allow the government to process and understand the threats and better assist corporations in dealing with the challenge. Yet, a key missing piece in the policy debate is just what the government will accomplish with such information.

Voluntary sharing mechanisms with the federal government have existed for quite some time, and yet the nation still finds itself presented with significant challenges. To truly address the issue in an effective fashion, new legislation should impose requirements on the government and Congress should create new mechanisms for assessing the Executive Branch's own performance in effectively combating this threat, permitting swift changes where success is not readily apparent.

Additional Requirements Needed

Improved information sharing, if handled properly, is a laudable goal and regardless will, in some part, become law. But to be truly successful, Congress should consider adding additional requirements for government action in conjunction with any such sharing.

Such requirements might include some of the following.

Tailored Government Feedback

The DHS should be required by law to assess information within an analogous, short window of time, and provide tailored, responsive information to corporations as feedback to the submissions they make.

Rather than the more generic information bulletins that generally are issued, companies should see the benefit of their participation and the government should be required to deliver meaningful and specific results.

Coordinating Government Campaigns

Rather than having agencies acting within siloed authorities on cybersecurity, Congress should mandate a multi-agency cell that brings information and interagency resources to bear via specific campaigns against targeted threat actors.

Such campaigns would likely need to be coordinated through the National Security Council's Deputy National Security Advisor for Cybersecurity to avoid bureaucratic turf battles that could limit campaign effectiveness, and will also need to contemplate certain changes to information-sharing requirements and tweaks to federal authorities.

Empower U.S. Cyber Command to Fight Back

We in the general public may not need to be privy to details as to whether and how U.S. Cyber Command (USCC) is taking steps against ransomware actors, but Congress should ensure the nation's policy interest is clear by funding programmatic offices within the USCC authorized with the specific task of combating actors targeting the U.S. private sector.

Specifically, the USCC must be charged with imposing specific costs on group and individual cyber actors, changing such actors' risk calculus and mercilessly hounding them into submission.

Review, Assessment, and Sunset

Congress should establish an independent review and assessment mechanism that is tied to a sunset clause in the information sharing program requirements.

The Executive Branch should be held accountable for the authorities it has been granted in imposing significant administrative costs on cyber victims at a time when it is challenging to deal both with foreign malicious and domestic regulatory actors.

The review mechanism should specifically assess, on a regular basis (i) what the government did with the information provided to it; (ii) the specific, tailored value that the government provided back to private sector entities; and (iii) the effectiveness of the measures taken in enabling recovery by victims and/or thwarting malicious actors.

The measures of effectiveness should be tied to an annual sunset/extension of the authority to push more proactive and effective efforts by government organizations empowered with significant compulsory powers.

Liability Protection

The current draft legislation refers to certain liability protections, but also commands the DHS to compare mandatory cyber event filings with public companies' regulatory filings. While the intent may be to ensure anything publicly reported is also submitted to the DHS, the perception will be the opposite—that the government is out to find any way possible to impose regulatory penalties on the private sector.

Full liability protections akin to those available in the Cybersecurity Information Sharing Act of 2015 should be available to parties compelled to file information.

Clarify Lines of Authority

Private parties encountering a cyber event are currently confronted with a range of federal agencies claiming to provide assistance and authority over such events. Congress must clarify the roles of various agencies specific to cyber events, focusing resources and authority on agencies best-positioned to affect positive outcomes.

The legislative and regulatory tone set by the inevitable information sharing requirements will make all the difference in whether they become a vehicle for true cooperation or a pastiche of check-the-box minimalism. In addition to the contemplated reporting requirements, Congress should act now to impose a range of obligations on the federal government to become more effective in the fight.

This column does not necessarily reflect the opinion of The Bureau of National Affairs, Inc. or its owners.

Freshfields Bruckhaus Deringer

Author Information

Brock Dahl is counsel in the Washington, D.C., and Silicon Valley offices of Freshfields Bruckhaus Deringer LLP, where he focuses on guiding clients through complex cybersecurity, advanced technology development, data privacy and strategy, and regulatory issues. He previously spent several years with the National Security Agency.