MIAMI-DADE FRIDAY, SEPTEMBER 24, 2021

OFFICIAL COURT NEWSPAPER OF SOUTH FLORIDA
DailyBusinessReview.com
An ALM Publication VOL. 96, NO. 66 $2.00
DAILY BUSINESS REVIEW

Bipartisan Bill to Require Certain Companies to Disclose Cyber Attacks

Commentary by Steven Reardon


Reardon

Leaders of the Senate Intelligence Committee, including Sens. Mark Warner and Marco Rubio, and a group of bipartisan lawmakers have recently introduced legislation requiring federal contractors and critical infrastructure groups to report attempted cyber breaches. The legislation, known as the Cyber Incident Notification Act of 2021, comes in response to a number of high-profile cyber attacks on critical infrastructure and federal contractors. Chief among these are the attacks on SolarWinds and Colonial Pipeline.

In December 2020, the IT management firm SolarWinds fell victim to a cyber attack, which resulted in the compromise of hundreds of federal agencies and private sector companies' private information. Then, in May 2021, there was a ransomware attack on the Colonial Pipeline, which halted pipeline operations temporarily and resulted in fuel shortages along the east coast. Florida has not been immune from such attacks. In early July, a ransomware breach of a Florida-based IT firm affected more than 200 businesses.

Typically, such attacks involve hackers gaining access to a business's electronic files; encrypting them, thereby denying the business access to its files; and seeking a ransom in exchange for the return of the files. Under existing law, there is currently no federal requirement for individual companies to disclose that they have fallen victim to a cyber attack or to ransomware. This is true even for businesses that contract with the federal government. The Cyber Incident Notification Act of 2021, however, seeks to change that.

The Cyber Incident Notification Act of 2021 introduces a new disclosure requirement for federal agencies, most federal contractors, and critical infrastructure providers to notify the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency ("CISA") within 24 hours of an identified breach of their cybersecurity systems. The Director of the Cybersecurity and Infrastructure Security Agency shall respond within two business days and coordinate a response to the cyber threat. Any new information regarding the cyber attack shall be provided to the CISA within 72 hours. The form of these notifications will be addressed in subsequent regulations, should the Cyber Incident Notification Act of 2021 be signed into law.

BOARD OF CONTRIBUTORS

While the act does not provide an exhaustive list of all covered entities, it does explicitly apply to federal agencies; federal contractors, other than those providing custodial services or providing products or services unrelated to information technology below a certain threshold; and owners and operators of critical infrastructure. Critical infrastructure is defined as "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters." Stated differently, the act is targeting large entities that are critical to national security, the economy, and public safety. This is further underscored by the definition of "cybersecurity intrusion," which, among other things, must involve "demonstrable harm to the national security interests, foreign relations, or economy of the United States or to the public confidence, civil liberties, or public health and safety of people in the United States."

The act also incentivizes companies to notify the Cybersecurity and Infrastructure Security Agency in the event of a cyber attack. In addition to receiving recommended actions to mitigate the impact of the cyber attack, covered entities that comply with the notice requirements in the act will be immune from suit from any person or entity, except for the federal government. Moreover, the information provided to the CISA will be exempt from public records requests and will not be used against the providing entity in any civil or criminal action. Thus, shareholders could not gain access to the disclosed information to use as evidence in a lawsuit. It also would require the CISA to anonymize personally identifiable information, so that companies can report incidents quickly and allow the government to act efficiently where needed. However, those entities who fail to comply will open themselves up to liability and may be assessed civil penalties by the CISA, not to exceed 0.5% of the entity's gross revenue from the prior year for each day the violation continues.

The act also directs the CISA to submit an annual report detailing the notifications it has received regarding cyber attacks, mitigating actions it has taken, and whether different types of entities should be required to submit cybersecurity notifications. Thus, which entities are subject to the notification requirement may change from year to year depending on trends in cybersecurity and which types of entities are being targeted.

In sum, the act seeks to open channels of communication between covered entities suffering from a cyber attack and the federal government so that they may coordinate an appropriate response to protect and to mitigate any damage to the national security, national economic security, or public health or safety. As highlighted by these lofty goals, the act will likely only apply to federal agencies, entities that contract with the federal government, or that provide critical infrastructure (such as pipelines and power plants). Notably absent from the proposed legislation is any requirement that these covered entities obtain a certain level of cybersecurity to stave off these attacks.

In Florida, most private sector employers will not fall under the purview of the act and will not be required to change how they respond to cyber attacks. However, it bears repeating that this bill is still in its nascent form and is subject to change prior to full Senate vote.

The Florida legislature recently enacted the Information Technology Security Act in an effort to enhance cyber security of state agencies. The act directs the Department of Management Services to develop best practices for cyber security and to implement a statewide cybersecurity plan for identifying, reporting, and mitigating cyber attacks. Like its federal counterpart, the Florida law does not apply to private sector employers. With that being said, all businesses should evaluate their vulnerability to cyber attacks and take measures to mitigate against potential attacks.

Steven Reardon is an attorney with the Miami-based law firm Allen Norton & Blue, a statewide firm devoted exclusively to the practice of labor and employment law. Contact him at sreardon@anblaw.com.