New Federal Tools Can Help Private Sector Protect Trade Secrets From Cyberattacks – And May Soon Require Reporting

Insights
4.02.21

Cybersecurity was undoubtably on the forefront of the agenda for many organizations in 2020 – and 2021 should be no different. The rapid shift to remote work over the past year has led to an increased number of cybersecurity threats for many organizations. A major risk that companies face when their information is improperly accessed through a cyberattack is the acquisition and potential misappropriation of trade secrets and other confidential and proprietary information.

It has largely been up to individuals in the private sector to protect their trade secrets from cyberattacks in the absence of a national response. However, going forward in 2021, the federal government has enhanced its response in preventing private-sector cyberattacks by initiating a process whereby it can work with the private sector to prevent them from occurring. By including the private sector in its cybersecurity defense plan, the government has departed from its historical approach which had until now focused solely on national security efforts.

New Federal Law Offers Aid to Private Sector

The William (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021 was enacted into law on January 1, 2021. The comprehensive legislation prescribes changes to the country's cyber defenses, reshaping how the private sector can combat growing threats as well as realigning the roles and responsibilities of federal government agencies. Essentially, this legislation has created an additional tool for companies to protect their trade secrets and proprietary information from theft and misappropriation through cyberattacks.

A key provision of the Act provides for the reestablishment of the Senate-confirmed National Cyber Director (NCD) within the Executive Branch. One of the main objectives of the NCD would be to act as the key intermediary with the private sector on all cyber issues. This office would serve as the central resource for information and policy guidance for the private sector. In fact, the statute calls on the NCD to "coordinate and consult with the private sector leaders on cybersecurity issues to better prevent cyberattacks."

Another key provision authorizes the Department of Homeland Security's (DHS) Cybersecurity & Infrastructure Agency (CISA) to issue administrative subpoenas to internet service providers that would compel them to provide information necessary to identify and notify an entity at risk of a cyberattack. This power is intended to streamline the information-sharing process between the

government and the private sector regarding known or unknown cyber vulnerabilities and emerging threats. This would allow the federal government to receive and release information on identified vulnerabilities.

The new law authorizes the CISA to take steps that will allow it to collect real-time threat information to share more rapidly with the private sector. It further calls upon the Government Accountability Office to issue a report analyzing the ways to improve the cybersecurity insurance market to assess and identify any barriers to underwriting cybersecurity risks. Moreover, the law directs DHS to develop a strategy to standardize all U.S.-based email providers on the same "Domain-based Message Authentication, Reporting, and Conformance" standard to secure emails from spam, phishing attacks, and ransomware. The standard is defined as "an email authentication, policy, and reporting protocol that verifies the authenticity of the sender of an email and blocks and reports to sender fraudulent accounts."

Potential Legislation on the Horizon

Congress is currently debating whether to require companies in the private sector to report incidents and if so, which incidents. The Biden administration is also working on ensuring a public-private partnership to defend again cybersecurity threats. In fact, Congress is slated to roll out proposals regarding cybersecurity incident sharing in the coming weeks. One bipartisan bill may be introduced to require certain incidents to be reported to the government. Given recent high-profile cyberattacks and period of regulation, it is likely that at least one of the bills will pass with overwhelming support.

How You Should Prepare

You may want to consider taking steps so that you will be able to take advantage of resources that have become available pursuant to the new statute. You may want to develop a cybersecurity framework and risk management plan if you do not already have one – with the assistance of legal counsel and IT security professionals. This framework should include gathering as many details as possible if an incident occurs so that you will be ready to provide a report (if one is eventually required). Further, by preparing a strategy and communication plan for responding to cyberattacks, you will be better able to take advantage of further federal assistance as it becomes available.

A Chief Information Security Officer can be instrumental in implementing and monitoring the above strategies. If a full-time CISO is not an option, part-time positions can be a feasible alternative, either as employees or on a consulting basis providing a pre-set number of hours of services per month. Since data protection monitoring is a constant effort, it is worthwhile to make this investment upfront to protect your trade secrets from cyberattacks.

Service Focus

Litigation and Trials

Litigation and Trials

Employee Defection and Trade Secrets