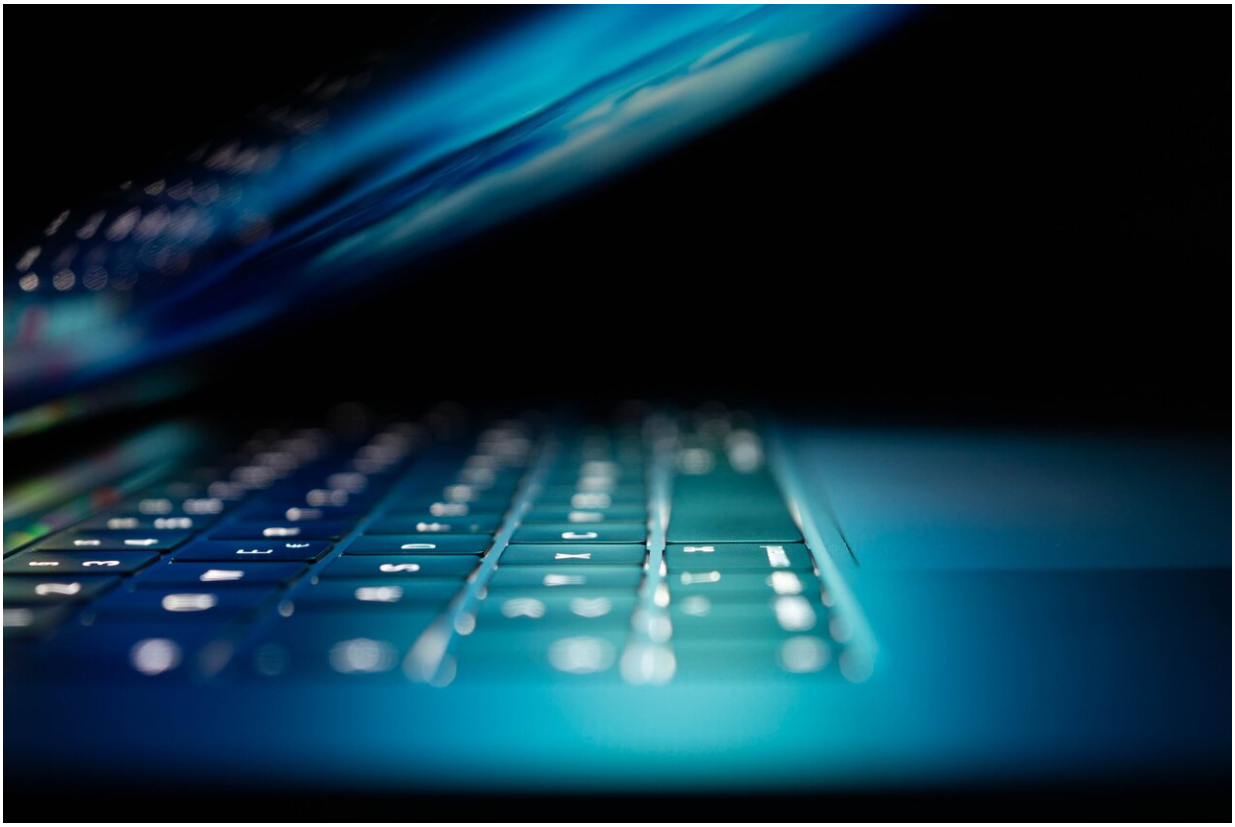
SolarWinds hack may lead to breach notification law and stronger cyber agency

March 3 2021, by Gopal Ratnam



Credit: Unsplash/CC0 Public Domain

One of the lesser-known aspects of the SolarWinds hack that lawmakers and top U.S. cybersecurity officials are grappling with is figuring out how many American companies and federal agencies have been

affected.

At present, no one knows.

This blind spot stems from the absence of a federal breach notification law that requires companies and federal agencies to notify the U.S. government if they have been hacked. That, however, may be about to change as congressional committees learn more about the SolarWinds hack and lawmakers in both chambers have signaled a bipartisan willingness to consider the idea.

Last week, lawmakers summoned top tech company executives and the CEO of SolarWinds, the company whose software became the conduit for Russian intelligence agencies to access thousands of American companies and federal agencies.

SolarWinds was hacked by Russian operatives who injected malware into routine software updates that went out to as many as 18,000 government entities and Fortune 500 companies that were clients of SolarWinds. Top U.S. government officials have said Russian intelligence services were behind the attack and that, as of now, nine federal agencies and about 100 companies were exposed but more victims are likely to be found as the probe continues.

Executives from FireEye, the cybersecurity company that found the Russian attack and made it public in December, Microsoft and SolarWinds told members of Congress that while they had come forward to share details of the attack, they were not obligated to do so and wanted Congress to address that gap.

Without a law and clear guidance, companies don't know whom to alert when they're hacked, Brad Smith, president of Microsoft, said at a joint hearing of the House Oversight and Reform and House Homeland

Security committees.

Companies also face a legal barrier because contracts with federal agencies "restrict a company like Microsoft from sharing with others in the federal government when a particular agency has been hacked in this way," Smith said.

In December, after FireEye revealed the SolarWinds hack and Microsoft began examining the breach among its federal clients, the company had to "go to each agency, tell them that we had identified that they were a victim of this. And then we had to say, 'You need to go over to this person in this other part of the government to let them know.' … We cannot do that for you."

House Homeland Security Chairman Bennie Thompson, D-Miss., said that in the absence of federal law requiring information sharing, tech companies are unable to discuss breaches and attacks with members of Congress or the Cybersecurity and Infrastructure Security Agency, known as CISA.

Rep. John Katko, R-N.Y., said the absence means there's "an undeniable gap in our country's cybersecurity posture," leaving companies without "a consistent overarching incentive for industry to disclose a breach." As a result, "federal agencies are often operating in the dark instead of having access to the critical aggregate data regarding the tactics, techniques and procedures of bad actors," he said.

FireEye CEO Kevin Mandia told lawmakers that state laws requiring notification of data breaches address only loss of personally identifiable information of consumers. In the case of the SolarWinds attack, since no personal information was lost, companies weren't obligated to even report the attack.

When a large-scale attack like the SolarWinds hack is discovered, few companies want to be the first to blow the whistle, Mandia said, noting that FireEye had come forward to reveal the information out of concern for national security.

Congress has tried and failed to pass a federal breach notification law before. Most recently, the House version of the Pentagon's fiscal 2021 policy bill included a provision added by former Rep. Cedric L. Richmond that would have required the Department of Homeland Security to establish a cyber incident reporting program overseen by the CISA. The measure won overwhelming bipartisan approval.

But the measure failed to pass the Senate and did not become law after the U.S. Chamber of Commerce objected and called for its rejection. The chamber said the amendment, which was offered during floor debate in the House, did not go through "regular order" in committees and that forcing companies to report breaches "undercuts public-private cybersecurity collaboration" and voluntary sharing of information.

In light of the SolarWinds attack, there's renewed interest in Congress to enact a federal law requiring breach notifications, Thompson said.

Rep. Michael McCaul, R-Texas, who previously served as chairman of the House Homeland Security Committee, said he was working with Rep. Jim Langevin, D-R.I., one of the members of the Cyberspace Solarium Commission, on a draft law that would require notifications of cyber intrusions. Under his proposal, companies could redact details of sources and methods as well as identifying details but still share baseline information on breaches and threats with CISA, McCaul said.

The Solarium Commission, a bipartisan high-level study group, recommended in March 2020 that Congress enact a federal law mandating notification.

Any cyber incident reporting system should include liability protection for companies so they are not subject to lawsuits when they share details of a breach, Chris Roberti, senior vice president for cybersecurity policy at the Chamber of Commerce, said in an email exchange. The House version of the 2021 Pentagon policy bill did not include such a provision, he said.

The chamber also has sent letters to House and Senate Intelligence committees asking them to pass legislation that would standardize intelligence-sharing efforts between "critical infrastructure" operators and the government, Roberti said.

When the Senate Intelligence Committee held a hearing on the SolarWinds hack in February, Sen. Mark Warner, D-Va., chairman of the panel, said it was time for Congress to consider new legislation.

"I would ask if we shouldn't have mandatory reporting systems, even if it requires some liability protection (for companies) so we can better understand and better mitigate future such attacks," Warner said.

Tech executives have also told lawmakers that CISA should be put in charge of securing the computer networks of the entire federal government outside the military, which is handled by the U.S. Cyber Command.

A majority of the 137 federal agencies lack the wherewithal to "execute a comprehensive cybersecurity strategy," Dmitri Alperovitch, executive chairman and founder of Silverado Policy Accelerator, a public policy organization focused on cybersecurity and national security, told the House Homeland Security Committee last month.

Putting CISA in charge of the effort by expanding its budget and giving it power beyond its current advisory-only capacity would yield better

outcomes, Alperovitch said.

©2021 CQ Roll Call
Distributed by Tribune Content Agency, LLC

Citation: SolarWinds hack may lead to breach notification law and stronger cyber agency (2021, March 3) retrieved 19 April 2024 from https://techxplore.com/news/2021-03-solarwinds-hack-breach-notification-law.html

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.