ML STRATEGIES

Hearings on the SolarWinds Hack and Possible Policy Responses

March 04, 2021 | | By **Christian Tamotsu Fjeld**

The 117th Congress kicked off its First Session with, among other initiatives, oversight hearings on the SolarWinds cyber hack. On February 23, the Senate Intelligence Committee held a **hearing** on the high profile, far-reaching breach; followed by a joint hearing on February 26 in the House of Representatives held by the Oversight and Reform and Homeland Security Committees. At both hearings, Sudhakar Ramakrishna, President and CEO of SolarWinds, Kevin Mandia, CEO of FireEye, and Brad Smith, President and Chief Legal Officer of Microsoft, testified. In addition, George Kurtz, the President and CEO of Crowdstrike, testified at the Senate Intelligence hearing, while Kevin Thompson, the former CEO of SolarWinds, testified in front of the joint House hearing. Together, the hearings represent what will likely be the first of several congressional forays into the SolarWinds hack, including possible legislative initiatives to address future possible incidents and supply chain security.

Background

To recap, SolarWinds is an information technology (IT) company (based in Austin, Texas) that provides products to business customers and the federal government enabling them to monitor and manage their IT networks. In December, the cybersecurity firm FireEye revealed that hackers, likely from Russia (if not the Russian government itself), exploited a suite of SolarWinds' network monitoring and management tools, Orion, to distribute malware throughout the IT networks of SolarWinds customers. Specifically, the hackers used Orion's update system – which sends out network software updates and patches – to create entry vectors, known as "backdoors", to surreptitiously infiltrate SolarWinds' IT management platforms. Once inside, the malware, known as "SUNBURST", was able to effectively execute new commands and exfiltrate files by disguising its activities as innocuous traffic indistinguishable from other data flows within the infected networks. This went on for at least nine months until FireFly's discovery.

While the entire universe of those affected by the hack is unknown, SolarWinds estimates that 18,000 of its over 300,000 customers are vulnerable to this malware. The *New York Times* **estimates** that as many as 250 government agencies and companies may have been affected. Furthermore, the intent of the Russian hack remains unknown – was it an espionage campaign to glean information or a more malicious attack meant to do harm? The effects of the breach remain similarly elusive; it is still unclear whether Russian hackers control critical operational elements of infected networks. Many cybersecurity experts believe that the same backdoor method used by hackers to infiltrate the SolarWinds platform can be used on other IT networks that use a similar suite of tools as Orion.

The SolarWinds hack is the latest in a series of decades-long, high profile cyber and data breaches that have compromised the security of government agencies and corporate America, as well as the privacy of millions of Americans. Over the last several years, Congress has passed numerous laws to improve the American posture on cyber attacks and supply chain security. Laws such as the **Cybersecurity Enhancement Act**, the **Federal Information Security Monetization Act (FISMA)**, the **Cybersecurity Information Sharing Act (CISA)**, and the **Internet of Things (IoT) Cybersecurity Improvement Act** have all addressed cybersecurity weaknesses by codifying the National Institute of Standards and Technology's (NIST's) development of the ***Cybersecurity Framework***, establishing the Department of Homeland Security's (DHS's) authority over the cyber practices of federal agencies, providing liability protection to incentivize the exchange of threat information, and developing federal standards for the use of federally procured IoT devices, respectively. Yet, despite these important laws, the hearings last week on the SolarWinds hack indicated that Congress is poised to take further legislative action.

Policy Considerations

At both the Senate and House hearings, Members largely focused their questions on what happened, the extent of the damage, and how Congress can help prevent future incidents from occurring again. From these questions, several policy themes emerged with varying degrees of Member and witness support. First, Members and witnesses generally agreed that the nation needs a larger, better-trained cyber workforce. Second, many attendees agreed that more resources must be dedicated to hardening the nation's cyber defenses, be it more federal government investment or updating the antiquated software and security systems of much of the nation's critical infrastructure. Congress can presumably address these policy areas in annual spending bills or in an infrastructure package.

Third, many Members focused on the need for better "cyber hygiene" and "best practices", which increasingly may include the practice of "threat hunting". Threat hunting is the proactive practice of constantly searching for cyber threats within a network. **According to Crowdstrike**, threat hunting entails "dig[ging] deep to find malicious actors in [an] environment that have slipped past [the] initial endpoint defenses" by using threat data and intelligence to discern new hacking tactics and techniques, as well as leveraging advanced data analytics and machine learning to detect unusual activities. NIST's Framework already outlines cybersecurity best practices appropriate for a whole range of stakeholders, large and small, and threat hunting could likely be part of the Framework's next edition (currently going through revision). While Congress tucked into its December spending package provisions of the **DHS Cyber Hunt and Incident Response Teams Act** – which directs DHS to maintain cyber hunt and incident response teams to aid government and non-government entities upon request – more can likely be done to incentivize the widespread practice of threat hunting.

Fourth, many Members and witnesses expressed the need for better "public-private partnerships" to address pervasive cybersecurity threats. Such collaboration has multiple policy dimensions. The notion that the federal government and private stakeholders should work together on cybersecurity is nothing new. In fact, the foundation of NIST's Framework is a public-private cooperation that has developed voluntary security guidelines almost universally lauded as an effective, practical, flexible, and evolving blueprint of cyber-hygiene that can be adopted by critical infrastructure stakeholders.

Furthermore, as part of that public-private partnership, both Members and witnesses expressed the need for a more robust exchange of relevant information. Some expressed support for a central federal agency to which the private sector reports (though specifics on how that central agency would be different from, say, DHS's Cybersecurity and Infrastructure Security are unclear), and many attendees at the hearings expressed at least qualified support for mandatory reporting requirements to the federal government. Such information-sharing includes providing threat intelligence to similarly situated, private stakeholders in order to maximize the speed and efficacy of the collective response to threats.

On several occasions, witnesses expressed concerns over legal liability and "victimizing victims" in the wake of a high-profile breach. On this note (and as noted above), CISA, which Congress passed in 2015 as part of an omnibus spending package, already confers liability protections on companies to encourage them to share information on "cyber threat indicators" and "defensive measures" to federal, state and local governments, as well as other companies. The sharing of such information must comply with the protocols set forth under CISA. At the hearings, witnesses did not specifically discuss how CISA could be further amended to make the law more effective, but Mr. Smith (of Microsoft) cited a lack of certainty over whom to report such breaches and further stated that government contracts restrict third-parties from sharing information with other government agencies. Furthermore, a September 2020 DHS Inspector General report found that CISA and the law's implementing agency, the aforementioned **Cybersecurity and Infrastructure Security Agency** (also known as CISA), had made progress in spurring increased information sharing through participation in the **Automated Indicator Sharing (AIS)** program. However, the IG report also found that the quality of the shared information was lacking. The report recommended, among other things, that CISA (the agency) take steps to increase the number of participants in the AIS program in order to improve the quality of the shared information and reduce the threat of attacks. How Congress will amend existing law to either expand or strengthen liability protections to coax a more robust exchange of threat incident data (or in exchange for more stringent, mandatory reporting requirements) is unclear.

ML Strategies will continue to monitor Congressional activity on cybersecurity legislation and oversight.

Authors

Christian Tamotsu Fjeld, Senior Vice President

Christian Tamotsu Fjeld is a Vice President of ML Strategies in the firm's Washington, DC office. He assists a variety of clients in their interactions with the federal government.