Wake-Up Call: What the SolarWinds Cyberbreach Means for Midstream Companies

By Krystal Pfluger Scott and Ewaen Woghiren, Jones Walker

In December 2020, various US government branches, including the departments of Defense, State, Commerce, and Treasury, were targeted in a massive espionage attack, potentially exposing confidential and classified information. The hack is now widely attributed to a Russian intelligence group known as "Cozy Bear," among other names. Ultimately, the hack impacted almost 200 organizations worldwide, including government agencies as well as consulting, telecom, technology, oil and gas, and even cybersecurity companies.

Although SolarWinds' full breach anatomy would exhaust both this article's scope and its readers' attention, everyone in the energy space needs to understand two things: First, the hackers gained access to their targets through software provided by a third-party company, an infrastructure monitoring and management platform call Orion, developed by Austin, Texas-based company SolarWinds. In what is known as a "supply chain attack" (similar to those used in the Target and Equifax breaches), when an organization updates to the compromised versions and malicious code enters its system, it allows hackers to obtain user rights and move freely within the network.

Second, the hackers started this process in September 2019—15 months before anyone discovered the breach. The hackers had more than a year to hack the third-party company, compromise the software build, and deliver trojanized updates to 18,000 customers before anyone figured this out. Let that sink in.

The cybersecurity world has long warned that nation-state actors will target the energy space. But the SolarWinds breach should shock the midstream sector, in particular, from any complacency because this space relies extensively on third-party providers for a broad range of services.

In a recent report on the state of cybersecurity in the midstream oil and gas space, Jones Walker LLP surveyed 125 key midstream executives to better-understand their cybersecurity readiness. That report found that only about half of companies contractually required their third-party contractors to adhere to data-security protections, only a minority required such contractors to supply written data-security plans, and few tested their vendors' cybersecurity plans. SolarWinds reminds us that a company's cybersecurity is only as good as the cybersecurity of its third-party providers.

Hackers' top priority is infiltrating systems. Most hackers gain access to and then stalk a company's networks for almost a year before revealing themselves, giving them time to identify the assets and user information they want. The SolarWinds breach was no exception to this rule. Cybersecurity and breach response preparedness thus warrant both proactive leadership involvement and early allocation of financial resources.

Not all cybersecurity measures are budget busting. Indeed, our survey found that some of the most effective, least-expensive strategies (such as training, data encryption, two-factor authentication, and cyber-insurance coverage) were woefully underutilized.

Ultimately, the SolarWinds breach is no surprise. What is surprising is the scope of the breach. The US government, for all its desire to do so, cannot fully protect our nation's critical infrastructure from nation-state hackers. Each company and individual must take responsibility to understand their own networks and address their unique cyber vulnerabilities.