The SolarWinds hack was all but inevitablewhy national cyber defense is a 'wicked' problem and what can be done about it

February 9 2021, by Terry Thompson

Military units like the 780th Military Intelligence Brigade shown here are just one component of U.S. national cyber defense. Fort George G. Meade Public Affairs Office/Flickr

The SolarWinds hack was more than just one of the most devastating cyber attacks in history. It was a major breach of national security that revealed gaps in U.S. cyber defenses.

These gaps include inadequate security by a major software producer, fragmented authority for government support to the private sector, and a national shortfall in software and cybersecurity skills. None of these gaps is easily bridged, but the scope and impact of the SolarWinds attack show how critical they are to U.S. national security.

The SolarWinds breach, likely carried out by a group affiliated with Russia's FSB security service, compromised the software development supply chain used by SolarWinds to update 18,000 users of its Orion network management product. The hack, which allegedly began in early 2020, was discovered only in December when cybersecurity company FireEye revealed that it had been hit by the malware. More worrisome, this may have been part of a broader attack on government and commercial targets in the U.S.

Supply chains, sloppy security and a talent shortage

The vulnerability of the software supply chain—the collections of software components and software development services companies use to build software products—is a well-known problem in the security field. In response to a 2017 executive order, a report by a Department of Defense-led interagency task force identified "a surprising level of foreign dependence," workforce challenges and critical capabilities such as printed circuit board manufacturing that companies are moving offshore in pursuit of competitive pricing. All these factors came into play in the SolarWinds attack.

SolarWinds, driven by its growth strategy and plans to spin off its managed service provider business in 2021, bears much of the

responsibility for the damage, according to cybersecurity experts. I believe that the company put itself at risk by outsourcing its software development to Eastern Europe, including a company in Belarus. Russian operatives have been known to use companies in former Soviet satellite countries to insert malware into software supply chains. Russia used this technique in the 2017 NotPetya attack that cost global companies more than US$10 billion.

SolarWinds also failed to practice basic cybersecurity hygiene, according to a cybersecurity researcher. Vinoth Kumar reported that the password for the software company's development server was allegedly "solarwinds123," an egregious violation of fundamental standards of cybersecurity. SolarWinds' sloppy password management is ironic in light of the Password Management Solution of the Year award the company received in 2019 for its Passportal product.

In a blog post, the company admitted that "the attackers were able to circumvent threat detection techniques employed by both SolarWinds, other private companies, and the federal government."

The larger question is why SolarWinds, an American company, had to turn to foreign providers for software development. A Department of Defense report about supply chains characterizes the lack of software engineers as a crisis, partly because the education pipeline is not providing enough software engineers to meet demand in the commercial and defense sectors.

There's also a shortage of cybersecurity talent in the U.S. Engineers, software developers and network engineers are among the most needed skills across the U.S., and the lack of software engineers who focus on the security of software in particular is acute.

Fragmented authority

Though I'd argue SolarWinds has much to answer for, it should not have had to defend itself against a state-orchestrated cyber attack on its own. The 2018 National Cyber Strategy describes how supply chain security should work. The government determines the security of federal contractors like SolarWinds by reviewing their risk management strategies, ensuring that they are informed of threats and vulnerabilities, and responding to incidents on their systems.

However, this official strategy split these responsibilities between the DOD for defense and intelligence systems and the Department of Homeland Security for civil agencies, continuing a fragmented approach to information security that began in the Reagan era. Execution of the strategy relies on the DOD's U.S. Cyber Command and DHS's Cyber and Infrastructure Security Agency. DOD's strategy is to "defend forward": that is, to disrupt malicious cyber activity at its source, which proved effective in the runup to the 2018 midterm elections. The Cyber and Infrastructure Security Agency, established in 2018, is responsible for providing information about threats to critical infrastructure sectors.

Neither agency appears to have sounded a warning or attempted to mitigate the attack on SolarWinds. The government's response came only after the attack. The Cyber and Infrastructure Security Agency issued alerts and guidance, and a Cyber Unified Coordination Group was formed to facilitate coordination among federal agencies.

These tactical actions, while useful, were only a partial solution to the larger, strategic problem. The fragmentation of the authorities for national cyber defense evident in the SolarWinds hack is a strategic weakness that complicates cybersecurity for the government and private sector and invites more attacks on the software supply chain.

A wicked problem

National cyber defense is an example of a "wicked problem," a policy problem that has no clear solution or measure of success. The Cyberspace Solarium Commission identified many inadequacies of U.S. national cyber defenses. In its 2020 report, the commission noted that "There is still not a clear unity of effort or theory of victory driving the federal government's approach to protecting and securing cyberspace."

Many of the factors that make developing a centralized national cyber defense challenging lie outside of the government's direct control. For example, economic forces push technology companies to get their products to market quickly, which can lead them to take shortcuts that undermine security. Legislation along the lines of the Gramm-Leach-Bliley Act passed in 1999 could help deal with the need for speed in software development. The law placed security requirements on financial institutions. But software development companies are likely to push back against additional regulation and oversight.

The Biden administration appears to be taking the challenge seriously. The president has appointed a national cybersecurity director to coordinate related government efforts. It remains to be seen whether and how the administration will address the problem of fragmented authorities and clarify how the government will protect companies that supply critical digital infrastructure. It's unreasonable to expect any U.S. company to be able to fend for itself against a foreign nation's cyberattack.

Steps forward

In the meantime, software developers can apply the secure software development approach advocated by the National Institute of Standards and Technology. Government and industry can prioritize the development of artificial intelligence that can identify malware in existing systems. All this takes time, however, and hackers move

quickly.

Finally, companies need to aggressively assess their vulnerabilities, particularly by engaging in more "red teaming" activities: that is, having employees, contractors or both play the role of hackers and attack the company.

Recognizing that hackers in the service of foreign adversaries are dedicated, thorough and bar no holds is important for anticipating their next moves and reinforcing and improving U.S. national cyber defenses. Otherwise, SolarWinds is unlikely to be the last victim of a major attack on the U.S. software supply chain.

Provided by The Conversation