BRIDGET McCREA | Contributor

Cybersecurity: A Top Supply Chain Concern

With several high-profile attacks taking place over the last few months, companies are rethinking their cybersecurity approaches to avoid potential breaches.

The Colonial Pipeline ransomware attack was just one in a recent series of cyberattacks on the world's organizations and governments, and a definite wake-up call for any organization that hasn't thought seriously about cybersecurity in a while.

Even with the ongoing pandemic, supply chain shortages and persistent labor gaps all keeping procurement leaders up at night, the need for strong cybersecurity protocols and procedures remains high. According to *The Economist*, more than one-third (36%) of global organizations reported cyberattacks "significantly" disrupted their supply chains in the last three years. And cyberattacks were second only to COVID-19 as the force wreaking havoc with the world's supply chains in 2020.

Knowing that their networks may be vulnerable to cybersecurity threats of any size or shape, companies now are thinking beyond the pandemic and reimagining their cybersecurity approaches.

Back-to-Back Strikes

The Colonial Pipeline ransomware attack followed pretty closely on the heels of December's SolarWinds hack, which allowed foreign hackers to spy on private companies like cybersecurity firm FireEye and the upper echelons of the US government, including the Department of Homeland Security and Treasury Department, *Business Insider* reports.

The pains associated with these cybersecurity breaches are both costly and impactful. According to IBM, the global average cost of a data breach in 2020 was $3.86 million, with the U.S. recording the most expensive average of any country at $8.64 million. For the Colonial Pipeline attack, the company reportedly paid a $4.4 million ransom to be able to restore its pipeline operations, the *Wall Street Journal* reports.

On average, IBM says organizations can save $1 million by containing a breach in less than 200 days, but the problem is that it takes an average of 280 days to identify and contain these attacks. About half of all breaches are caused by malicious attacks, with compromised credentials and cloud misconfigurations each responsible for 19% of malicious breaches.

The Government Hits Back at the "Bad Actors"

Not willing to see its critical systems and the nation's infrastructure attacked by cybercriminals, the U.S. government is taking steps to help strengthen its stance against what the cybersecurity world refers to as "bad actors."

In May, President Joe Biden signed an executive order outlining more rigorous cybersecurity requirements for software providers that contract with the federal government. The administration also launched a series of 100-day initiatives to improve cybersecurity in critical infrastructure, including the electric grid and oil and gas pipelines.

Also, the Homeland Security Committee recently passed a number of bills focused on preventing future cyberattacks. The Pipeline Security Act, for example, aims to bolster the Transportation Security Administration's role in responding to attacks on pipelines.

According to the *Washington Post*, the panel advanced four other bills, including one to identify risks in critical supply chains and another focusing on cybersecurity vulnerabilities that would give the U.S. government the power to create an incentive-based program that allows industry, individuals, academia and others to compete in identifying remediation solutions for cybersecurity vulnerabilities.

Another bill establishes a grant program for state, local, and tribal organizations to address cybersecurity risks and cybersecurity threats, while a final one is focused on a National Cyber Exercise Program for testing cyber readiness and responses to incidents, the publication reports.

5 Steps to Better Cybersecurity

Of course, it doesn't take a wide-sweeping, headline-making cyberattack to bring a company—and possibly even its customers and suppliers—to its knees. Even a minor hack, phishing attack, or other crime can severely impact a company's ability to operate. *In Supply & Demand Chain Executive*, GEP's Aryaman Sethi outlines some of the top strategies that companies can use to thwart cybersecurity threats.

1. **Identify where the risk lies.** Conduct a thorough evaluation of your supply chain partners and understand what data is being shared with whom. "Ensure maximum security and limit your data exposure by establishing where unnecessary data is being shared," Sethi advises. "Minimize access to cloud servers storing important information."
2. **Secure supplier contracts.** Incorporate security into the contract from the very start and be clear about what information is required and by whom. Ensure only limited access to third-party vendors (with third-party vendor misuse being one of the biggest security threats today).
3. **Conduct vulnerability mitigation and testing.** By running vulnerability scans, you can identify various security concerns such as poor password choices or bad database configurations and mitigate the level of risk for various fragments of the supply chain.
4. **Encrypt data.** Sethi advises that all protected customer information should be contained in encrypted and secure files that are constantly updated to keep pace with the newest technologies.
5. **Establish incident response protocols.** Be ready to respond to cybersecurity incidents by having a plan in place. "By preparing a handy template to record all key aspects of an incident to ensure consistency, readily available forensic imaging tools and the contact details of all key stakeholders to ensure quick outreach," Sethi writes, "you can minimize the damage from an attack."