Watch Your (Supply) Tail

This article was originally published on The Huffington Post on September 30, 2014.

by Brian E. Finch

Brian E. Finch
Public Practices
+1.202.663.8062
brian.finch@pillsburylaw.com

Brian E. Finch is a partner in Pillsbury's Public Policy practice in Washington, DC. He is a recognized authority on global security matters and is a leader of the firm's Global Security Services team.

"My logisticians are a humorless lot," Alexander the Great once commented. "They know if my campaign fails, they are the first ones I will slay."

Wow. Here I thought I had worked for some tough bosses in my day, but yikes.

His point about logistics is quite valid, however. Logistics in warfare can easily make the difference between victory and defeat. In World War II, the allied landings in North Africa were so badly planned from a logistical perspective that the battle was nearly lost as soon as it began. Poorly loaded supply ships resulted in a plethora of useless goods like tent pegs and typewriters while ammunition and vehicles were hopelessly misplaced.

Eventually the logistical Achilles Heel was remedied, and victory was achieved. But the lesson remains the same - if you cannot get troops and material to the fight, the fight can quickly be lost.

That is why a **report** from the Senate Armed Services Committee really caught my attention this week. In that report, the Senate detailed how various contractors for the U.S. military's Transportation Command (TRANSCOM) had been the subject of repeated and serious cyber intrusions in a period spanning 2012 through 2013.

The attacks, of which there were approximately 50, were highly sophisticated and often undetected by the contractors. Drilling down even further, at least 20 of the attacks were attributed to Chinese actors. Yet, out of all of the attacks, only twice was TRANSCOM alerted to the fact that its contractors were breached.

These attacks were not random or happenstance. Rather, they fit directly into China's well-known strategy of disrupting an enemy's logistics and mobilization capabilities. This is a particularly serious issue when the U.S. military is involved, as it relies on "precision in coordinating transportation, communications, and logistics networks."

In other words, the American military relies on precise timing and movement as part of its battle plan. Disrupt that, and its capability to conduct a fight is seriously diminished.

Uh oh.

The Senate noted some other serious worries, such as the fact that some contractors allegedly failed to notify TRANSCOM of cyber-attacks even though they were contractually

obligated to do so. Also, the Federal Bureau of Investigation was apparently aware of a number of the breaches, but because of a breakdown in intra-governmental communications it did not notify TRANSCOM or the Defense Department writ large of the attacks.

To me the larger point illustrated by this Senate report is that no facet of a government agency, or a private business for that matter, is "safe" from cyber-attacks. The cost of conducting cyber-attacks is so small when compared to the potential rewards, and the incredible availability of sophisticated tools makes such attacks basically a given at this point.

Additionally, the private sector should think long and hard about this attack and how it could impact them. Even if a company does no business with the U.S. government, the fact that cyber criminals are probing logistics networks to potentially disrupt supply chains is very disturbing.

Certain countries are well-known for using cyber-attacks for pure economic gain. There is no reason to think that this tactic of infiltrating the logistical base will not be used to create an advantage in the business world. So many businesses utilize "just in time" deliveries for components and raw materials, so any disruption could be disastrous from a reputational or financial perspective. Imagine the business harm that could result if a product is not reliably available ... customers could quickly turn elsewhere for alternative products, and it may be very difficult to win that business back.

The lesson here is that every company should examine the cyber vulnerabilities of its logistics network. Disruptions are quite possible, and companies need to factor that in to their planning in order to minimize potential consequences.