Enabling better Cybersecurity Information Sharing with Small and Medium-sized Partners

August 31, 2017

By Jeff Brown

"Information sharing" is one of the most powerful tools organizations can use against cyber threats that can erupt without warning and cause disruption worldwide.

Once an organization—any organization, whether public or private sector—spots the tell-tale patterns of a new attack, alerting other organizations of these warning signs can help halt the spread in its tracks. However, proactive information sharing is only as good as the underlying mechanism used to share it.

In the defense industrial base (DIB), formalized policies and procedures for information sharing between organizations − and with the Pentagon − go back nearly a decade. And they're working, to a degree. Hacking major defense contractors or the Department of Defense is no easy task, and industry members actively cooperate to ensure it stays that way.

But, in the past decade, information-sharing practices have left behind a vital part of the DIB: small- and medium-sized partners. It's one of the major problems with cybersecurity today. We all know we need to share, and we all say we want to, but a significant part of the supply chain is left out for structural − not policy − reasons.

These information sharing mechanisms assume that participants have sophisticated operations in place, with sufficient personnel on hand to vet, assess, and produce cyber threat data and implement pertinent countermeasures via a sophisticated security infrastructure. Small- and medium-sized businesses rarely have these capacities. They can neither contribute to, nor ingest the data the way it is currently produced and shared.

However, leaving out small- and medium-sized businesses leaves everyone at risk. These companies are embedded into the defense supply chain where they're sources of innovation and new technologies themselves, as well as holding much of the same critical information attackers are failing to get from the larger companies. As a result, attackers are targeting smaller suppliers, perceiving them, rightly or wrongly, as an easier way to get to the same critical data they can no longer get from the larger companies.

The problem is compounded by a culture of secrecy where many of those who produce the valuable data place more emphasis on keeping what they know confidential than on helping protect the broader, less capable industrial base. Where to draw the line between secrecy and sharing can be debated with good arguments on both sides. But, until institutions collectively find a better balance, cyber criminals and nation-state industrial espionage forces will continue to exploit this vulnerability. They know that small- and medium-sized businesses may never get the word on an attack the large companies have already detected and stopped.

So, how do we close the gap? Our smaller partners need an automated system that does the network defense for them − something that protects them without anyone needing to think about it. A system

patterned after the antivirus model could work, even if it applies to different matters, such as blocking the domains or IP addresses of a cyber-attack campaign's command-and-control channels.

The Pentagon should help us partner with industry to create a broader information-sharing environment tailored to small and medium businesses that is both affordable and passive. It should be focused on attacker command-and-control channels to make it suitable for a perimeter or cloud activity. Such a system might not be well suited for the most sensitive data, but the benefit of sharing most of the data more broadly outweighs the downside of withholding the 10 percent that's too sensitive for wide dissemination.

Jeff Brown serves as the Vice President and Chief Information Security Officer for Raytheon Company (NYSE: RTN), with over 30 years of experience in the Communications and Information Technology field.