In a Cyber-attack, Should We Shoot Back? A DHS Cyber- Official Weighs In

Posted At : November 21, 2013 1:55 PM | Posted By : John Slye
Related Categories:

At an industry event I participated in recently, a current U.S. Department of Homeland Security cybersecurity official was asked whether he thought private companies should be legally permitted to respond to cyber-attacks with in-kind force to protect themselves and their customers, similar to having an armed guard on duty capable of shooting an on-coming attacker. The question recognizes a hot topic in cybersecurity – what is the role and scope of active and reactive defenses and who should use them? The official's response took some by surprise and got everyone's attention. And it revealed the complex world of cybersecurity in which we find ourselves.

This **event on Continuous Monitoring** inaugurated a series by the Chertoff Group to discuss the challenges and implications of agencies shifting from periodic or annual security and compliance assessments to risk and mitigation efforts assessed in real- or near-real-time. Participants included several former DHS leaders including Undersecretary for Cybersecurity Mark Weatherford, Chief Information Officer Richard Spires, Deputy Secretary Jane Holl Lute, and Secretary Michael Chertoff.

One current DHS participant was John Streufert, Director of Federal Network Resilience and who leads DHS's **recently awarded** $6 billion Continuous Diagnostic and Mitigation (CDM) program. Streufert was part of a panel with leaders from several cybersecurity companies discussing how to successfully implement continuous monitoring.

During the Q&A a question came from the audience asking Streufert and his fellow panelists their opinion on whether companies should be allowed to respond or retaliate against cyber-attackers, similar to having an armed guard on duty that is capable of shooting an attacker. Streufert's response was emphatic:

> *"When considering whether we want to encourage companies to respond in kind when they are attacked we need to ask a fundamental question. Do we really want to trust people who are incapable of securing their **own** networks to be accurate and effective at "shooting back" when they are attacked? I don't think so."*

Streufert's fellow panelists, as well Lute and Chertoff later, agreed with Streufert and added their perspectives that can be summarized in a couple of basic points that drive home the complexity of the issue.

- **Attribution is hard** – Attackers are keenly adept a concealing their identities, origins and tracks, so knowing exactly who hit you and from where is an ongoing challenge that cyber-defenders face. Given that, any "return shots" could actually result in high collateral damage to innocent people and systems that are only cursorily related to the attack. In fact, setting up an unwitting down-stream victim might even be part of the assailant's plan.
- **Calling the cops *is* a real response** – Companies are not alone, left to fend for themselves or left without remedy. Federal, state, and (most) local law enforcement agencies all have channels to investigate cyber-attack incidents. Companies need to be willing and forthright in sharing with law enforcement information about the attacks they incur. If you're concerned about liabilities, trade secrets, negative publicity or corporate privacy discuss the matter with your corporate legal counsel beforehand so that you can share confidently.

In this age of increased interconnectivity among organizations and individuals, governments and businesses, we are learning that we're never that far-removed from malicious actors who seek to do us harm, for whatever reason. As progress is made in continuous monitoring for cyber-vulnerabilities and attacks maybe we will reach a point where the need for proactive and reactive measures is made unnecessary. If Streufert's comments, and those expressed by others, are indicative of the challenges still ahead, then we'll continue to see the same essential question raised for the foreseeable future.

---
*Originally published for Federal Industry Analysis: Analysts Perspectives Blog. Stay ahead of the competition by discovering more about **GovWin FIA**. Follow me on Twitter **@GovWinSlye**.*