CYBER SECURITY SPECIAL

CIOReview

JUNE -12 - 2015 CIOREVIEW.COM

In My Opinion

Enrique Salem,
MD, Bain Capital Ventures
(Former President & CEO of
Symantec [Nasdaq: SYMC])

Open Inference:

Combating Intrusion in Real Time using Big Data

Mike Pollard,
Co-Founder & CEO

Scott Streit,
Co-Founder & Chief Scientist

$ 15US SE 12

CIO REVIEW
44790, S Grimmer Blvd.
#202, Fremont, CA-94538

Nuala O'Connor

Why Offensive Countermeasures Weaken Our Cybersecurity

By Nuala O'Connor, President & CEO, Center for Democracy & Technology

For many fortunate Americans, cyber attacks and malicious hacking lives only in the headlines. When salacious details from private email conversations at a movie studio are posted online, we might snicker and wonder how someone could be so careless. But when a major retailer has their payment systems breached, it can quickly become all too real and personal.

The fact is that cyber attacks on corporations, networks, and individuals are increasing. According to an HP study released in October 2014, companies have experienced a 144 percent increase in successful cyber attacks. Another study from the Center for Strategic and International Studies estimates that global cyber crime costs the economy $445 billion annually.

The economic impact and the threat to personal privacy have rightfully led to calls for improved cybersecurity measures in the U.S.. Congress has taken up a number of legislative efforts to increase coordination and companies are working to strengthen their internal protections. These are important and necessary efforts, but there is a troubling response that has entered into the cybersecurity debate: offensive countermeasures.

You can think of offensive countermeasures as "hacking back" at cyber attackers. In the cybersecurity context, countermeasures are technologies that can respond to an attack, either offensively by seeking out and hacking the attacker directly or defensively by setting up traps inside a network or information system that respond to limit damage or annoy attackers. In short, either create walls to stop an attack, such as a firewall or honeypots, or if someone attacks you, attack them back. The former is already legal under current law, and frequently employed by companies today. The latter is where the real problems come in, and where real harms are likely. The harms are also likely to impact a much broader community than the intended target.

Offensive or retaliatory cyber countermeasures are generally prohibited under current law, specifically the Computer Fraud and Abuse Act. This is a good thing, because there are a myriad of serious problems with a company launching offensive countermeasures. While countermeasures may be designed to prevent harms, such as ones aimed at deleting stolen data or deploying "helpful worms" that could automatically remove malware and fix vulnerabilities, the possibility of unintended consequences is real and severe.

The most obvious problem is that when it comes to cyber attacks, determining exactly who the attacker is can be incredibly difficult. Attackers regularly route attacks through innocent parties and botnets to hide their identity, which greatly increases the risks of any offensive countermeasure harming individuals or networks that were not the source of the cyber attack. This means that a "hack back" approach could unknowingly take down the network at a hospital, school, or government facility or even critical infrastructure used to route power or water, or to transport people. The reality is, once a malicious software or vulnerability is introduced, there's a good chance it will go viral.

There is also a very real risk of rapid escalation of problems with offensive countermeasures. If a private company responds to a cyber attack, it's possible they could "hack back" at a foreign government and create a broader international incident. Many attribute the infamous Sony hack to North Korea, so this scenario is not nearly as far-fetched as it may initially sound. While the internet may not recognize traditional state boundaries, the impact of rogue cyber actions can certainly have traditional diplomatic repercussions.

While the primary focus of cyber security legislation currently being considered is on enhancing information sharing, all of the major bills currently being considered in Congress include new authorizations for countermeasures, often euphemistically called "defensive measures." The Cybersecurity Information Sharing Act (CISA, S. 754), the Protecting Cyber Networks Act (PCNA, H.R. 1560), and the National Cybersecurity Protection Advancement Act (NCPAA, H.R. 1731) all authorize operation of countermeasures. While the bills state that these countermeasures must be deployed on one's own network and contain other limitations, CISA and the NCPAA fail to prohibit countermeasures that have external effects, potentially opening a Pandora's Box of reckless activities detrimental to global computer security. PCNA does a better job by only authorizing countermeasures whose effects are limited to one's own information system, but still raises concerns by preempting all law, including the Computer Fraud and Abuse Act, a step that appears both dangerous and unnecessary.

> "While the internet may not recognize traditional state boundaries, the impact of rogue cyber actions can certainly have traditional diplomatic repercussions

Quite simply, responsible cybersecurity legislation should not include any authorization for countermeasures. The White House information-sharing proposal released in January of this year wisely adopts this policy stance.

As companies and governments consider the best way to enhance cybersecurity to protect their systems, constituents, and customers, their focus should remain squarely on narrowly tailored information sharing procedures and strengthening the core security of their own network infrastructure. Also, both government and corporate employees should be trained to avoid phishing scams, easily crackable passwords, and other basic security vulnerabilities that all too often create the initial opening for aggressive cyber attacks.

The instinct to punch back is undeniable, but in the cyber world it is far better to focus on having the best security in place and a good response plan developed, rather than introducing well-intentioned malicious programs into cyberspace. Congress should resist the urge to create any legislation that invites companies to "hack back" and companies should avoid entering into cyber battles that may escalate beyond their control. Cybersecurity requires a collective, cohesive commitment to strengthening the infrastructure of the internet, which is something not accomplished through endorsement of offensive countermeasures. CR