Cybersecurity Information-Sharing Legislation: Going on the 'Defensive'—Separating Fact From Fiction

October 5, 2015

Some privacy and civil liberties groups perpetuate the claim that S. 754, the Cybersecurity Information Sharing Act of 2015 (CISA), authorizes businesses to use offensive measures or "hack back." The Protecting America's Cyber Networks Coalition (the coalition), which represents 50 leading associations of nearly every sector of the America economy, is pushing the Senate to pass CISA in October. Both the coalition and most policymakers reject the falsehood that opponents of CISA try attaching to the bill.

Businesses need to use 'defensive measures' in real time to mitigate cyberattacks.

First, CISA does not permit so-called hacking back—companies are not permitted to destroy or render computer systems unusable. The bill ensures that defensive measures are properly confined to a business' own networks or to those of its customers. Given the scope and sophistication of malicious cyber behavior, the private sector seeks to secure its own systems and networks against nation-states and other hostile actors in a responsible manner. Companies and organizations do not seek to act in a way that traditionally has been the province of defense, law enforcement, and national security agencies.

The coalition strongly backs CISA so that businesses may better defend themselves and their customers. Industries play a central role—because they have to—in spotting and responding to cyber aggressions against their own networks and information systems located in the United States.[1] Boards and senior executives devote billions of dollars toward protecting their sensitive business and consumer data.

The definition of defensive measure in CISA excludes destructive, harmful actions.

(7) DEFENSIVE MEASURE.—

(A) IN GENERAL.—Except as provided in subparagraph (B), the term "defensive measure" means an action, device, procedure, signature, technique, or other measure applied to an information system or information that is stored on, processed by, or transiting an information system that detects, prevents, or mitigates a known or suspected cybersecurity threat or security vulnerability.

(B) EXCLUSION.—The term "defensive measure" *does not include a measure that destroys, renders unusable, [provides unauthorized access to],*[2] *or substantially harms* an information system or data on an information system not belonging to—

(i) the private entity operating the measure; or

(ii) another entity or Federal entity that is authorized to provide consent and has provided consent to that private entity for operation of such measure [italics added].

Second, the coalition is confident that the vast majority of policymakers in Congress and the administration interpret the definition of a "defensive measure" in CISA as it is intended—businesses should be permitted to take defensive actions to stop cyberattacks.[3] The legislation does not give organizations (including even privacy advocacy groups) the green light to go on the offensive or hack back against cyber

[1] www.whitehouse.gov/the-press-office/2015/02/11/remarks-prepared-delivery-assistant-president-homeland-security-and-coun

[2] Provided here in brackets, section 2(7) of the managers' amendment to CISA clarifies that the authorization to employ defensive measures does not allow an entity to access a computer network without authorization.

[3] See pages 5–6 of CISA, as reported, www.congress.gov/114/bills/s754/BILLS-114s754pcs.pdf.

intruders, which critics of CISA wrongly contend. What's more, the bill creates narrowly crafted liability protection to spur companies' sharing of cyber threat data. But this safeguard does not extend to defensive measures. Also, the widely circulating managers' amendment to CISA clarifies that companies are not allowed to gain unauthorized access to a computer network.

Third, it is worth providing the Senate Intelligence Committee's views regarding defensive measures.[4] The bipartisan committee report to CISA, which passed the panel by a vote of 14 to 1 in March, shows that lawmakers do not intend defense measures to damage or substantially harm another party's computer networks. The bill ensures that defensive measures are properly bounded. What's significant, but frequently overlooked, is that coalition members believe that CISA does not grant them the go-ahead to hack back.

Senate Intelligence Committee to businesses: 'You have a right to self-defense.'

The term "defensive measure" is defined as an action, device, procedure, signature, technique, or other measure applied to an information system or information that is stored on, processed by, or transiting an information system that detects, prevents, or mitigates a known or suspected cybersecurity threat or security vulnerability. However, a defensive measure *does not include a measure that destroys, renders unusable, or substantially harms* an information system or data on an information system not belonging to the private entity operating such measure or another entity or Federal entity that is authorized to provide consent and has provided consent to that private entity for operation of such measure.

Recognizing the *inherent right of self-defense* that entities have to protect their networks and data, the [Senate Intelligence] Committee intends for this definition to provide a positive legal authority allowing private entities to take measures to take appropriate steps to defend their own information networks and systems, or those of their customers when authorized by the written consent of such customers, against malicious cybersecurity threats. For example, a defensive measure could be something as simple as a security device that protects or limits access to a private entity's computer infrastructure or as complex as using sophisticated software tools to detect and protect against anomalous and unauthorized activities on a private entity's information system.

Regardless, this definition *does not authorize the use of measures that are generally to be considered "offensive" in nature*, such as unauthorized access of or executing computer code on another entity's information systems or taking an action that would substantially harm another private entity's information systems.

The Committee is aware that defensive measures on one entity's network could have effects on other networks. It is the Committee's intent that the authorization in this Act extends to defensive measures on an entity's information systems that *do not cause substantial harm to another entity's information systems or data on such systems*, regardless of whether such non-substantial harm was intended or foreseen by the implementing entity [italics added].

CISA is prudent, self-defense legislation; overwrought criticisms of the bill fall flat under scrutiny.

The bottom line is lawmakers contend that businesses have an inherent right to self-defense, especially when the attackers are nations, criminal gangs, and ideologically motivated hackers or terrorists. CISA reflects the intuitive thinking that organizations should be informed about threats before they are assailed—not after the fact—and that entities should be able to guard themselves in appropriate ways. Frankly, given that bad actors are probing public- and private-sector networks every day to steal data for illicit gain or launch disruptive and destructive attacks, CISA is a restrained measure. Overwrought criticisms of the bill just don't hold up under reasonable examination.

[4] See pages 4–5 of the committee report, www.congress.gov/114/crpt/srpt32/CRPT-114srpt32.pdf.

Agricultural Retailers Association (ARA)
Airlines for America (A4A)
Alliance of Automobile Manufacturers
American Bankers Association (ABA)
American Cable Association (ACA)
American Chemistry Council (ACC)
American Coatings Association
American Fuel & Petrochemical Manufacturers (AFPM)
American Gaming Association
American Gas Association (AGA)
American Insurance Association (AIA)
American Petroleum Institute (API)
American Public Power Association (APPA)
American Water Works Association (AWWA)
ASIS International
Association of American Railroads (AAR)
Association of Metropolitan Water Agencies (AMWA)
BITS–Financial Services Roundtable
College of Healthcare Information Management Executives (CHIME)
CompTIA–The Computing Technology Industry Association
CTIA–The Wireless Association
Edison Electric Institute (EEI)
Electronic Payments Coalition (EPC)
Electronic Transactions Association (ETA)
Federation of American Hospitals (FAH)
Food Marketing Institute (FMI)
Global Automakers
GridWise Alliance
HIMSS–Healthcare Information and Management Systems Society
HITRUST–Health Information Trust Alliance
Large Public Power Council (LPPC)
National Association of Chemical Distributors (NACD)
National Association of Manufacturers (NAM)
National Association of Mutual Insurance Companies (NAMIC)
National Association of Water Companies (NAWC)
National Business Coalition on e-Commerce & Privacy
National Cable & Telecommunications Association (NCTA)
National Retail Federation (NRF)
National Rural Electric Cooperative Association (NRECA)
NTCA–The Rural Broadband Association
Property Casualty Insurers Association of America (PCI)
The Real Estate Roundtable
Retail Industry Leaders Association (RILA)
Software & Information Industry Association (SIIA)
Society of Chemical Manufacturers & Affiliates (SOCMA)
Telecommunications Industry Association (TIA)
Transmission Access Policy Study Group (TAPS)
United States Telecom Association (USTelecom)
U.S. Chamber of Commerce
Utilities Telecom Council (UTC)