BANK POLICY INSTITUTE

The President’s Cyber EO is a Strong Start. Now It’s Congress’s Turn to Act

Heather Hogsett | May 20, 2021

A string of recent high-profile incidents has made it clear our nation’s cybersecurity defenses are woefully inadequate. These events — starting with the SolarWinds compromise in December 2020, followed by the Microsoft Exchange Server hack and most recently the ransomware attack against Colonial Pipeline — illustrate two things: 1) it’s not a question of “if” but rather “when,” and 2) borders do not exist in cyberspace. Whether you are a small mom-and-pop shop, a large corporation or a government agency, even the most sophisticated organizations can be vulnerable.

The recent Executive Order (Order) on Improving the Nation’s Cybersecurity is a far-reaching and important step, but there is still more to be done, and Congress should pass complementary legislation to address remaining gaps. There is a need for greater action on the part of both private sector critical infrastructure owners and operators and the government to improve transparency when critical infrastructure data may be impacted by a breach. Congress also needs to create effective processes for collaboration between intelligence agencies and critical infrastructure.

CYBER DEFENSES DEPEND ON EVERY LINK IN THE SUPPLY CHAIN.

Despite banks’ own measures and robust regulatory oversight, a lack of transparency and real-time information on the operations and security measures of their service providers and other third parties remains a key challenge. In this regard, the Order is a welcome and positive development. Requiring all government agencies and their service providers to implement stronger security measures and share incident data will help raise the security bar for many businesses and other critical infrastructure sectors that have thus far left themselves, and those that depend on them, vulnerable to criminal hackers and nation-state attacks.

Many of these providers do not have the same legal and regulatory requirements as banks to protect customer data, so banks often become a kind of “default regulator” for other sectors as they negotiate operating and security requirements into contractual obligations. This can be a cumbersome and difficult task.

While some critical infrastructure entities directly serving federal agencies are covered by the Order, others fall outside its requirements. Ensuring that these firms are also subject to heightened cybersecurity expectations and independent oversight will be necessary for real progress to be made. Equally important will be requiring these entities to report cyber incident information to the government to help inform our nation’s collective defenses. Several members of Congress are drafting bills to require just that. The critical elements for success will include the following:

- making sure that the threshold for reporting information is high enough to avoid capturing so much information that it becomes useless,
- ensuring that the government can adequately protect this new treasure trove of data, and
- clarifying that the timelines for reporting do not interfere with crisis response efforts at the affected entity.

Banks and other financial institutions have been required to report cyber incidents for more than 20 years and recognize the value of providing timely information to benefit the entire financial sector. For this reason, firms have invested significantly in collaborative organizations like the Financial Services Information Sharing and Analysis Center, the Financial Services Sector Coordinating Council and the Analysis and Resilience Center that work to coordinate, analyze and share information on cyber risks across thousands of financial institutions. Firms coordinate regularly with the U.S. Treasury Department, the Cybersecurity and Infrastructure Security Agency, regulators and other government partners and are investing more time than ever addressing cybersecurity on the front line and in the boardroom. A recent survey conducted by BPI in coordination with McKinsey & Company found that the time spent on cyber in the boardroom continues to increase, with 95 percent of board committees reportedly discussing cybersecurity and technology risks four or more times per year.

MOVING FROM REACTIVE TO PROACTIVE.

Even with these efforts, impediments remain to addressing cyber threats, and Congress should act to ensure that government agencies that hold critical infrastructure information are held to the same standard as private industry. Current reporting requirements are one-directional and fail to account for the risks the government may pose to the operations of private critical infrastructure. As evidenced by the SolarWinds incident, it is equally important that government agencies have a duty to notify private entities when their data, or confidential private industry data that they hold, may be impacted by an incident.

Congress should also remove lingering barriers to collaboration between critical infrastructure and the intelligence agencies. Our adversaries look to exploit government and private sector systems and will target either or both to achieve their desired effect. Existing collaboration efforts are reactive to past events and focused on sharing best practices across all levels of government and the private sector. This is important work, but insufficient for certain industries and private entities that have been deemed critical to national security, in particular those identified by the 2013 Executive Order on Improving Critical Infrastructure Cybersecurity to be vital to national economic security[1].

As part of an effort to address our nation's cybersecurity challenges, Congress should enact the Cyberspace Solarium Commission's recommendations (5.1.1 and 5.1.2) to create a formal structure for the intelligence agencies to identify and incorporate the information needs of critical infrastructure to help defend against increasingly sophisticated foreign threats. Financial institutions have sought to improve collaboration with the intelligence agencies to better inform their unique foreign intelligence collection activities and leverage their analysis and early warning capabilities. Progress has been sporadic and inadequate given the severity of the threats we face.

If government and critical infrastructure can adhere to the same rigorous cybersecurity standards, truly partner together to share relevant, timely and actionable information, and remove barriers to collaboration as teammates, the U.S. will be better positioned to get ahead of threats, rather than perpetually running from behind. Recent events have underscored this need, and, fortunately, momentum is building in Congress to address it.

Disclaimer: The views expressed do not necessarily reflect those of the Bank Policy Institute's member banks, and are not intended to be, and should not be construed as, legal advice of any kind.

[1] The Order defines critical infrastructure as a system or asset that is "so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters."