GOVINFOSECURITY®

Cyber War Council Idea Wins Few Backers

Government Mute on Proposal to Defend Financial Institutions

By Eric Chabrow
July 8, 2014

An idea to create a cyber war council, reportedly proposed by a financial services industry trade group, has not received an enthusiastic reception from cybersecurity experts, some of whom question its viability to defend against crippling cyberattacks.

The Securities Industry and Financial Markets Association proposes a government-industry cyber council designed to help prevent terrorist attacks that could trigger financial panic, according to a news report from **Bloomberg** that the association declines to confirm.

The news report, citing an association internal document, says the group is calling for formation of a committee of financial industry executives and deputy-level representatives from at least eight U.S. agencies, including the Treasury Department, the National Security Agency and the Department of Homeland Security, all led by a senior White House official.

"If the aim is to make crisis response as routine as possible, as quickly as possible, then that is to be commended," says Ian Wallace, a visiting fellow for cybersecurity at the Brookings Institute's Center for 21st Century Security and Intelligence. "At a practical level though, institutionalizing an arrangement that requires eight deputy secretaries to meet with industry representatives seems like a bureaucratic nightmare."

A Dire Need?

SIFMA, according to the Bloomberg report, sketches a dire need for the war council. The report says the SIFMA document notes: "The systemic consequences could well be devastating for the economy as the resulting loss of confidence in the security of individual and corporate savings and assets could trigger widespread runs on financial institutions that likely would extend well beyond the directly impacted banks, securities firms and asset managers."

A SIFMA spokeswoman, Liz Pierce, refused to comment on the news report. Several other financial industry officials said they were unaware of the SIFMA proposal and declined to comment on it.

The news report was vague on how such a joint council would function, saying the government-industry group would develop plans for "much quicker, near real-time" dissemination of information from agencies to the private sector and ways to "actively defend the industry" if preparations for a cyberattack are discovered in advance. SIFMA is also seeking "pre-discussed and mutually understood protocols" for the industry to request government help during and after an attack, the report says.

SIFMA, which represents banks, securities firms and asset managers, has retained former NSA Director Keith Alexander to "facilitate" the joint effort, and Alexander, in turn, has brought in Michael Chertoff, the former DHS secretary who runs the consultancy Chertoff Group, according to Bloomberg.

Reached at his office, Alexander declined to comment on the report, saying he hadn't read the story. And spokespeople at the White House, NSA and departments of Homeland Security and Treasury also declined to comment on the war council proposal.

Harsh Assessments

But while government officials aren't talking, others aren't shy about sharing their opinions. "Of all the bad ideas I've heard doing this work, that is the worst of the bad ideas," says a veteran IT security operative who has held a variety of high-level **cybersecurity** positions in government and industry.

One reason this veteran security leader says the war council is a bad idea is that it would put American-based, global financial services companies in an awkward position of working with the U.S. government while seeking to sell digital financial services overseas.

After the United States established the U.S. Cyber Command in 2010 (see ***Gates Defines Military Cyber Command's Role***), about two dozen other nations established their own cyber commands. If a war council is implemented, the IT security expert says, other nations might create their own councils, which could create havoc in securing cyberspace.

Allan Friedman, co-author of the book ***Cybersecurity and Cyberwar: What Everyone Needs to Know*** and research scientist at George Washington University's Cybersecurity Policy Research Institute, also argues that the war council concept is a bad idea.

Alluding to the apparent involvement of Alexander and Chertoff, Friedman says the war council would lack support from privacy and civil liberties groups. He also says that U.S. government agencies have been extremely active for years, even decades, working toward a more secure and resilient American critical infrastructure, "often over the protests of SIFMA members."

"Before setting up yet another partnership simply by citing the same concerns that cybersecurity scholars and practitioners have known for years," Friedman says, "I

encourage SIFMA to actively identify what policies need to be changed and implemented."

Self Reliance

Jim Harper of the Cato Institute, a libertarian think-tank, also considers a war council a bad idea. "It is the responsibility of the financial services industry itself to secure its assets, and sloughing that responsibility off to the government is a disaster in the making," he says.

"The proposal is not driven by the merits, of course, but by the institutional need of SIFMA to grow its own enterprise," says Harper, a senior fellow at the institute. "If financial institutions take care of their own cybersecurity, SIFMA has very little role. If SIFMA organizes a public-private war council, they are at the center of the action and their fundraising stays high."

But Adam Segal, director of the digital and cyberspace policy program at the think tank Council on Foreign Relations, reserves judgment on the reported SIFMA proposal. He says that without more specifics, it's hard to say how the war council solves two of the problems that often come up in discussing cyberthreat information sharing.

"First, the private sector always complains that government does not push the right type of information out fast enough. [The war] council might solve that, might not," Segal says. "Second, there are still liability issues involved with private sector [organizations] sharing info with each other and with government, and you need legislation to address that, not a council."

The House last year passed the Cyber Intelligence Sharing and Protection Act, known as CISPA (see ***House Handily Passes CISPA***), but the White House threatened to veto it because it contends it didn't provide enough privacy protections and gave businesses that shared cyberthreat information too broad liability protections (see ***White House Threatens CISPA Veto, Again***).

On July 8, the Senate Intelligence Committee approved the Cybersecurity Information Sharing Act of 2014, like CISPA, legislation that is backed by the financial services industry but opposed by privacy and civil liberties groups (see ***Senate Panel OK's Cyberthreat Info Sharing Bill***).

Shared Mission

In a speech last month at the Gartner Summit on Information Security and Risk Management, White House Cybersecurity Coordinator **Michael Daniel** conceded it's tough for society to organize itself to defend against cyberthreats because all organizations function along the border of cyberspace (see ***Why Global Internet Governance is Tough***).

"Protecting cyberspace is, by its very nature, a mission shared by all. This reality makes organizing for cybersecurity incredibly complex, because it requires cooperation across boundaries in the physical world that are difficult to bridge - between government agencies, within the private sector, and between the government and the private sector," Daniel says. "If we all live and work at the border, how we communicate with one another - in our role as sentries and responders - is more important than ever. Developing broad partnerships to shore up our individual portions of the border is critical to both individual and collective success."