How a 'Bad Day' in Banking Bolsters National Security

And is setting the standards for protecting U.S. critical infrastructure.

Amanda Ziadeh

Thu, 08/02/2018 - 14:11

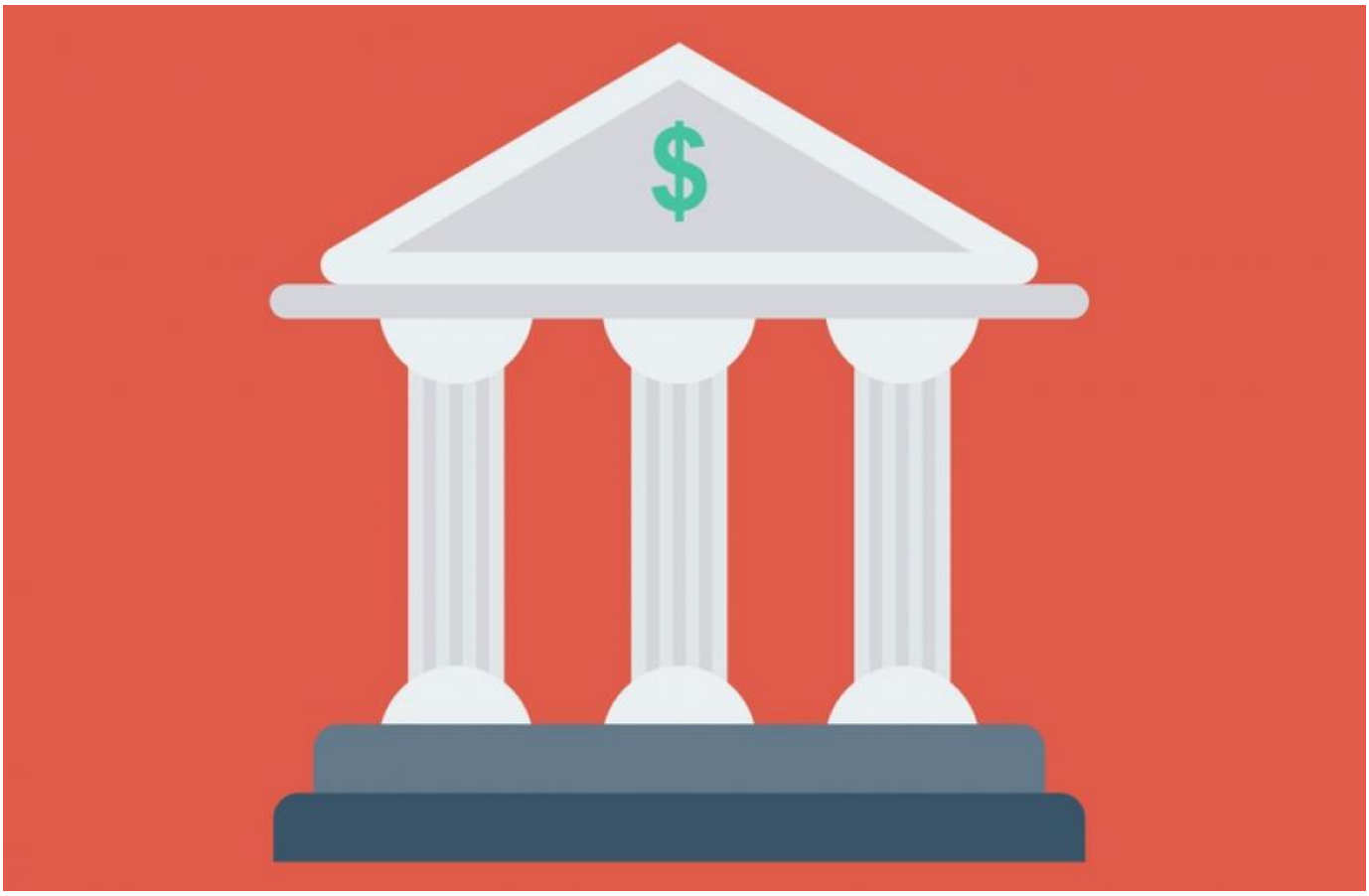

Illustration: dinosoftlabs/iStock

NEW YORK CITY — The Homeland Security Department's new National Risk Management Center replicates the model the financial sector has taken to move beyond information sharing and into consistent, collaborative threat analysis, and even the energy sector is following suit.

Let's Start with the Financial Sector

In 2016, CEOs of the country's top banks formed the Financial Systemic Analysis

and Resilience Center to identify, analyze, assess and collaborate on mitigating systemic cyberrisk to U.S. financial system. The center promotes operations and collaboration between participating firms, industry partners and the government.

“As a sector, we need to come together and prioritize our risk,” FSARC President and CEO Scott DePasquale said July 31 at the DHS National Cybersecurity Summit. The sector needed to decide what a “bad day” looked like, then understand and map the interconnectedness of all the financial systems, and “respond and recover before we ever get to protect and defend,” he said.

The financial sector needed a transparent process where it could work with government and sector-specific agency partners like the Treasury Department and DHS consistently, several times a month. FSARC calls that its Risk Committee, and prior, this process wasn’t happening around the concept of systemic risk.

So, these operators of “systemically relevant critical infrastructure,” as DePasquale described them, defined that bad day, created the playbooks and mapped out the critical processes underpinning these key systems that were exposed and how they’re connected. And even further, FSARC explored the technologies supporting those underlying systems.

If one of those critical national functions is compromised, there is a playbook for how the sector will work together. Government partners have been talked to and prepared in advance, and the tools that will make the sector measurably more resilient have been implemented. FSARC prioritizes its efforts around that bad day, creating strategic, early warnings of an adversary targeting critical assets.

And in many ways, DHS’ new center mimics the overall FSARC effort. Because rather than focusing on just information sharing, or disseminating the data as quickly as possible without context, FSARC builds context back up through framing and joint analysis.

That doesn’t happen at scale quickly, as DePasquale said.

“You have to protect and defend that data you’re asking people to share . . . and that takes time,” he said. Finding a way to do that while getting the sector and its partners to participate is evolutionary.

And it’s not just DHS following the lead of the financial sector.

Energy Also Goes Beyond Information Sharing

When the Energy Department received congressional authority to protect the energy sector from cyberthreats, its Undersecretary Mark Menezes looked to other sectors as example, and used the National Laboratories to help implement what had been observed.

“Information sharing . . . is important, but on the other hand, it’s identifying the threats and developing the technologies necessary to ensure that our energy system writ large is operational,” Menezes said, speaking on a panel with DePasquale

The energy sector is targeted more as the U.S. leads the world as a net exporter in oil and natural gas. And because most Americans expect their lights to turn on and gas stations to be full, safeguards must be in place to ensure the resiliency of the electrical systems.

“You cannot have electricity unless you have power,” Menezes said, and this requires a secure transmission system.

So, the national labs meet with members in the electricity, oil and natural gas sector coordinating councils to collaborate. And while Energy’s IT systems are able to identify and information share, it’s not quite enough. With the industrial control systems playing a key role in modernizing energy systems, Menezes said Energy needs to be able to go down into the supply chain, look at the devices used across the energy systems and identify and address those threats.

“We’re trying to do it as much as we can with what we have, but I know it’s been the financial industry that has been setting some of the standards,” he added.

It All Comes Back to Collaboration

So, Energy’s goal is to be more collaborative. For example, its Office of Cybersecurity, Energy Security, and Emergency Response houses the Cybersecurity Risk Information Sharing Program for situational awareness and information sharing; the Cybersecurity for the Operational Technology Environment for two-way

data sharing and analyses; and the Cybersecurity Testing for Resiliency of Industrial Control Systems.

“We can all really work together because we’re all interrelated and interdependent,” Menezes said, “and so the better we are . . . at guarding the turf and pulling together, I think we can make some great progress very quickly.”

And DePasquale found while relationships between the sectors and government are valuable alone, they have to turn into “routinized collaboration,” he said, and that’s why DHS’ National Risk Management Center is so important.

Information sharing is a transaction, but the center establishes a persistent set of joint, analytical collaboration to watch the impact of adversaries on the sectors, analyze vulnerabilities and threats.

View printer friendly version
Department of Homeland Security
Energy Department
FSARC
National Risk Management Center
critical infrastructure
financial sector
cyber
Federal Cybersecurity