Securities Industry News

April 10, 2006

It Takes a Community: You might need a scorecard to know all the players, but the financial industry has effectively used collective action to strengthen its "critical infrastructure"

BYLINE: Jeffrey Kutler

LENGTH: 2322 words

In the 1990s, amid a booming peacetime economy, the Clinton administration forced the financial services industry to take a close look at its vulnerability to external and operational threats and its ability to recover from disasters of any cause or proportion. The government had identified banking and finance as one of the critical infrastructures--others included telecommunications, energy, health care and transportation--of importance to national security, and now the weight of a 1998 presidential directive required highly competitive companies, spanning subsectors that rarely had reason to communicate with each other, to do just that.

Of course, financial institutions of all kinds--from the lowliest credit union to the most complex and sophisticated of securities markets--were always in the business of risk management and were no strangers to the concepts of security firewalls, business continuity planning and disaster recovery. Regulators and auditors made sure that contingencies were accounted for. But answering to the higher reaches of the executive branch in Washington required a mobilization of a different sort.

Trade groups from the American Bankers Association (ABA) and the Securities Industry Association (SIA) on down represented their members in dialogues primarily led by the Treasury Department. Bits, the technology division of the Financial Services Roundtable, which represents the biggest commercial banks, investment banks and insurance companies, became particularly influential because of its diversified membership. And in 1999 a new entity sprang up that was a direct manifestation of the newly raised consciousness about finance as a critical infrastructure: the Financial Services Information Sharing & Analysis Center (FS-**ISAC)**. A nonprofit then run by Science Applications International Corp. (SAIC), a consulting firm and federal contractor with close ties to the defense and intelligence establishments, it was one of more than a dozen sector **ISACs** with a mission of monitoring threats against networks and physical facilities around the clock and sharing and disseminating pertinent information among industry participants.

The FS-**ISAC** turned out to be just the beginning of a collective movement in infrastructure protection and resiliency that reached full flower after the Sept. 11, 2001 terrorist attacks. What happened on that day said at least two things to Donald Donahue, COO of the Depository Trust & Clearing Corp., itself a critical part of the securities processing infrastructure. One was that "everyone needs to understand how well the financial sector did on Sept. 11," Donahue said in a recent interview with Securities Industry News. He noted that even in the high-profile instance of the U.S. stock markets' closing down for four days, their systems and ability to transact were not impaired. Telecommunications connectivity to the floor of the New York Stock Exchange and the lack of physical access to that location were the reasons for the shutdown.

But therein lay the second conclusion: There was a need to go "beyond the state of the art," as Donahue put it. The Securities Industry Automation Corp. (Siac), for one, the joint technology venture of the NYSE and American Stock Exchange, built a new network based on inherently secure and resilient Internet protocol technology, the Secure Financial Transaction Infrastructure, that eliminates the "single point of failure" risk that plagued financial market connectivity on Sept. 11. In Chicago, about two dozen major financial institutions and marketplaces including the Chicago Board of Trade and Chicago Mercantile Exchange (CME) coalesced in a regional resilience effort called ChicagoFirst.

Those are just two examples of post-Sept. 11 mobilization; the activity is visible on the individual firm level, whether internally or in concert or collaboration with technology service providers, within and across associations and, topping off the hierarchy, at associations of associations. FS-**ISAC** is looking more and more like one of the latter. William Nelson, who became its executive director in February, says that its participation is about to rise by 50 percent, to 2,700 institutions, thanks to a deal he has worked out with America's Community Bankers, and he expects the number to approach 7,000 by year-end. The Leesburg, Va.-based **ISAC**--which this year brought in VeriSign Corp. to replace SAIC to run its operations center--has already penetrated the cream of the brokerage industry, said Nelson. "They are among our big dues-paying members--there may be as many as 50 people within a company receiving our alerts," he added. Suzanne Gorman, Siac's head of corporate information security, is chairman of FS-**ISAC.**

Super-Association

But the association of associations is a post-Sept. 11 initiative--the Financial Services Sector Coordinating Council (FSSCC), currently chaired by Donahue. (His interview with SIN, speaking in that capacity, is on page 16.) Name a banking, securities or insurance trade group, and it's probably in the FSSCC. So are the CME and ChicagoFirst, the Nasdaq Stock Market and New York Board of Trade, the Options Clearing Corp. (OCC), SIA and Siac. It forms a kind of counterweight to the Financial and Banking Infrastructure Information Committee, a who's who of regulatory bodies, which takes the collaborative notion up a notch by holding joint meetings with FSSCC three times a year.

"The relationship [with regulators] by definition involves some degree of tension," said Donahue, who is due to step down as chairman in June, in favor of OCC vice chairman George Hender. "That type of collaborative interaction is very new. It's one accomplishment of the last two years that will have enormous significance going forward."

FSSCC was formed in spring 2002, with Rhonda MacLean, then Bank of America Corp.'s chief information security officer and now CEO of Charlotte, N.C. consulting firm MacLean Risk Partners, as chairman. Donahue, who became chairman when MacLean's two-year term expired in 2004, also inherited an associated title--sector coordinator--that puts him at the table with government officials as the chief spokesperson for the industry's preparedness initiatives. Donahue said that on his watch, FSSCC has been focused on "baseline issues" such as raising the bar for telecommunications resiliency, improving crisis communications in cooperation with FS-**ISAC** and, as of late last year, supporting research and development programs. The FSSCC 2005 annual report said that the R&D agenda "will highlight research opportunities on topics such as secure and resilient networks and protocols, enrollment and identity-credential management, risk management and protection against insider threats--a mix of hard science' initiatives such as telecommunications engineering and soft science' efforts focusing on issues such as consumer behavior."

The council went into crisis mode--or into supporting its members' and their constituents' crisis responses--when Hurricane Katrina hit the Gulf Coast last August. It was "a graphic illustration of the interdependencies among critical infrastructure sectors," noted the annual report, as in the need to have adequate fuel supplies for transportation and power and telecommunications for operating the automated teller machines that were essential in getting cash to the population. Besides concrete efforts by banks to provide essential financial services and serve as conduits of financial assistance, "we also had to quash rumors that there was a cash shortage in the region," said Donahue.

In January, FSSCC made finance one of the first sectors to begin alerting its constituents to the avian flu threat. The council put out a 4,300-word paper on the business continuity issues and recommended responses, such as making preparations for telecommuting and teleconferencing and limiting staff travel. Donahue said at the time that the pandemic "remains a possibility, not a fact. While we do not want to create a sense of panic, FSSCC believes that heightened awareness and preparation is a prudent course. ... Business continuity planning needs to encompass the long-term and sometimes large-scale disruptions that an outbreak of avian flu might cause, and our aim is to help financial institutions in thinking through and addressing the issues their specific organization might face."

Physical and Cyber

Donahue acknowledged that the recent emphasis at FSSCC has been more on physical than on information or cyber-security matters, but the pendulum may be swinging back as the R&D committee gets to work. The committee's most concrete effort so far is working with Treasury on a technology-assessment test bed that could, according to the annual report, "include computational support, diverse connectivity options and data scrubbing and management as well as facilities for interaction and collaboration among researchers."

By contrast, FS-**ISAC** was created amid the Internet explosion, when cyber-security concerns such as computer viruses and denial-of-service sabotage were running high, but now its information-sharing and infrastructure-protecting charter encompasses "physical and cyber threats, vulnerabilities and events." Organizationally, many financial firms address physical and cyber security separately, though some now have the two security segments reporting to a single chief security officer. FS-**ISAC,** as an opinion leader, could help to push a more holistic view of security.

Nelson, who before joining the **ISAC** spent 18 years as EVP of electronic payments association Nacha, is careful to circumscribe the entity's role even as it broadens the view of its mandate. "We're not trying to build new projects," he said. "You won't see us developing two-factor authentication [see page 22]. ... We won't replace Bits or SIA or ABA in their relationships with members. But if those organizations want to be able to push a button and reach everybody they need to reach fast, then FS-**ISAC** would be the one to do that."

Nelson is setting in motion a strategic plan that includes membership marketing--the **ISAC** has a goal of "reaching the entire industry" and was 34 percent there at the time of a year-end letter to members from chairman Gorman--upgrading the VeriSign-run securities operations center and improving its alerting and analytical tools. Nelson oversees and participates in a constant stream of messages, calls and meetings while also attending and participating in events with other **ISACs,** with FSSCC and various constituent groups and government agencies to promote the cause.

"We could strengthen our development tools to make [information sharing among members] easier," said Nelson. "You can get so engrossed in remediating your own problem that you don't automatically think about telling the world about it--when it may be beneficial to do that," he went on. "The good thing about FS-**ISAC** is that you can be anonymous in sharing your information."

"People are willing to pool their information on cyber and physical threats, but there is still some concern about the news getting out," observed Daniel Schutzer, a long-time Citigroup technologist who now leads the Financial Services Technology Consortium (FSTC). "We're chipping away" at the resistance.

FSTC and Resiliency

Information sharing and collective action on noncompetitive issues is an even older tradition at the FSTC, which has more than 100 members from across the sector. Schutzer arrived as executive director in February after having founded the group in the early 1990s and participated in its programs as a Citibanker. The New York-based FSTC, which has close ties to Bits and FS-**ISAC** and is a FSSCC member, served as a unified industry voice on the technology underlying Check 21, the federal law that allows for image processing to speed up check collections, and has been promoting standards for what it calls "better mutual authentication" between the providers and clients.

Last month, the consortium announced the formation of an enterprise architecture standing committee to address common challenges in "regulatory compliance, technology risk management, integrating emerging technologies, linking technology architecture to business issues and managing the overall complexity of technology," Schutzer said. In February, FSTC said that 15 financial institutions and technology companies were participating in its resiliency model project, an attempt to set standards and benchmarks for institutions to measure and compare their resiliency and business-continuity-planning (BCP) effectiveness. In a related effort, the consortium is surveying and analyzing BCP-related rules and regulations around the world "and attempting to reconcile them--there is some unnecessary overhead," said Schutzer. "Even the Sarbanes-Oxley Act, which relates to the financial health of an organization, also has to do with security, resiliency and operational risk."

Schutzer believes that the industry as a whole has made major strides in addressing information security threats; collaboration and information sharing have even had an effect on the pesky phishing attacks and spoofing of company Web sites that have contributed to the identity theft epidemic.

Authentication solutions are on the horizon, though Schutzer pointed out that online identity frameworks such as Microsoft Corp.'s recently floated InfoCard are variants of "digital wallet" technologies that have been tried before, with little success. "We co-hosted a workshop with the World Wide Web Consortium and looked at InfoCard and some open-source equivalents," said Schutzer. "They could help, and maybe the timing is better now with the availability of broadband and new players that may have a broader reach than those in the past."

http://www.securitiesindustry.com http://www.sourcemedia.com

LOAD-DATE: April 7, 2006

LANGUAGE: ENGLISH

PUBLICATION-TYPE: Newsletter

JOURNAL-CODE: SIN