

6. FINANCIAL SERVICES LEARNING FROM SUCCESS

Since September 11, the cooperation between the financial services sector and government regulators has offered a glimpse of a process that promises to protect America's long-term economic security.

Because the health of the financial services infrastructure is critical to the health of our nation, coordination of crisis management efforts is a top priority among industry leadership. The commitment to financial security is seen in the numerous conferences, meetings, and tabletop exercises held by senior executives, including the recent Department of Homeland Security (DHS) sponsored multinational exercise *Cyberstorm*,¹ which brought financial services leaders together with top thinkers in other critical infrastructure industries, such as telecommunications, information technology, and energy as well as with legislators, regulators, and security experts, to test and evaluate the processes, procedures, and safeguards in place. The results of these efforts are robust emergency communication tools, strengthened industry resources, and documented lessons learned from disaster situations.

The industry's response to September 11 and subsequent recovery would not have been possible without the lessons learned from previous crises. While no one could claim to have been prepared for September 11, the efforts made to prepare the industry and promote resiliency allowed a coordinated response when disaster struck. Arguably, the quick response and recovery by the financial sector following the attacks gave the American public and the world a clear signal that our economy was stable and the assets of 270 million Americans were secure.

Though a highly competitive industry, financial services firms have been able to work together in noncompetitive forums to address emerging threats. A small pool of key industry associations including the Financial Services Sector Coordinating Council (FSSCC) and the

Financial Services Information Sharing and Analysis Center (FS/ISAC) are especially vital.

The FSSCC's mission is to act as a focal point for private-sector engagement with industry regulators, law enforcement, the Department of the Treasury, the Department of Homeland Security, and the Federal Reserve. The FSSCC then works in concert with the Treasury Department and other government agencies to address critical infrastructure and homeland security issues. It currently has thirty-three members representing 8,000 financial institutions ranging from BITS and the Financial Services Roundtable² to the New York Board of Trade and the American Bankers Association. Launched in 1999, FS/ISAC was established by the financial services sector in response to Presidential Directive 63 in 1998. That directive—later updated by Homeland Security Presidential Directive 7 in 2003—mandated that the public and private sectors share information about physical and cyber security threats and vulnerabilities to help protect U.S. critical infrastructure.³

Efforts by the financial services sector to improve preparedness highlight the utility of specific measures that are transferable to other sectors:

- ◆ improving communications during crises;
- ◆ building regional partnerships;
- ◆ enhancing the resiliency of telecommunications services;
- ◆ increasing the reliability of the electrical grid;
- ◆ tightening security of software, hardware, and the Internet; and
- ◆ intensifying oversight of third-party providers.

August, 14, 2003, the Northeast was hit with a devastating blackout. That day, BITS held a bimonthly meeting of senior executives of financial institutions in Detroit, at the headquarters of member company Comerica Incorporated. On the agenda was cyber security and critical interdependencies with the nation's telecommunications networks. At about 4:30 in the afternoon, lights in the conference room flickered and extinguished. It quickly became clear that the situation was not a momentary lapse. Through pagers, cell phones, and BlackBerries, the group learned within minutes that power was lost not just in Detroit, but also throughout much of the Northeast.

Executives immediately activated their company business continuity plans, including the BITS Crisis Communicator,⁴ a high-speed, automated alert system that allows financial services executives to communicate and coordinate with each other, government agencies, and other industry sectors. Within the hour, it became known that the blackout was not a terrorist act. This information helped executives to understand the scope of the incident and strike the appropriate note in messages to their personnel, customers, and the broader public.

Multiple conference calls throughout the evening had CEOs, CIOs, and crisis management executives from BITS member companies discussing effects to their institutions, the backup systems that had been activated, and the point at which power might be restored. In the absence of landline telephones and waning cell phone batteries, the BITS Crisis Communicator functioned as intended, providing members with a real-time forum to exchange information.

Several weeks later, BITS convened a series of conference calls to discuss lessons learned from the blackout. Backup systems had worked, alternate communication systems were used successfully, and there was no adverse impact on settlements and payments. Moreover, each institution had benefited from the cooperation and communication that took place among the financial services regulators, the Treasury Department, and the private sector via the BITS Crisis Communicator.

Donald Donahue, chairman of the FSSCC, testified to Congress that the post–September 11 environment was a strong impetus for improvements to resiliency and continued vigilance and coordination between financial entities. He stressed that beyond their efforts to share best practices broadly, trade associations have published recovery and resiliency guides such as the “BITS Guide to Business-Critical Telecommunications Services”⁵ and the “Report of the Assuring Telecommunications Continuity Task Force.”⁶ His testimony covered cyber security measures as well as physical security.

“The industry’s other ‘core clearing and settlement organizations’—handling payment and securities and derivative settlement transactions—have implemented a variety of steps since September 11 to reinforce the resilience of their operations, ranging from the same type of duplicated and regionally dispersed operations my company has implemented to reciprocal backup arrangements between organizations. . . . In addition, key trading markets have thought through reciprocal

arrangements permitting one market to trade another market's financial instruments in an extreme situation where the latter market was completely unable to operate."⁷

Donahue's comments were echoed in congressional testimony by Scott Parsons, the deputy assistant secretary for critical infrastructure protection and compliance policy at the U.S. Treasury Department. Chaired by the assistant secretary of the treasury for financial institutions, the Financial and Banking Information Infrastructure Committee coordinates the twenty agencies with regulatory powers throughout the financial sector. This group works to identify the interdependencies of the financial services, telecommunications, energy, and transportation sectors.⁸ Their efforts have also improved information sharing among federal, state, and local partners by publicizing a number of lessons learned through documents and impact studies.⁹ Together, these strategic public and private partnerships show how businesses engage in a collaborative effort to improve economic security and preparedness, particularly when backed up by strong federal leadership. Continuation of outreach and coalition building should remain a priority for both the Treasury and Homeland Security secretaries.

The Government Accountability Office (GAO) issued major reports in 2003¹⁰ and 2004¹¹ about the level of preparedness and potential for disruption of financial sector operations. Significant strides were made after the 2003 GAO assessments, which showed major vulnerabilities in continuity of operations planning. The financial sector began creating backup facilities at diverse locations separate from primary facilities, decentralizing key personnel, and increasing physical and information security measures. In order to improve resiliency, the industry has worked with the telecommunications and power sectors to outline its needs and develop plans for the restoration of critical communication services, including the creation of a private phone network for financial service providers. The importance of the telecommunications infrastructure to the security of the financial services sector has not been ignored by federal regulators and telecommunications providers who are working closely to improve the redundancy of the infrastructure. The 2004 GAO report also stresses the importance of the SEC mandating specific rules for the industry relating to business continuity as well as SEC requests for additional resources and personnel to conduct necessary audits on resiliency issues. Both Donahue and Parsons stress in their comments that

smart regulation, in concert with strategic public-private partnerships, increases the likelihood of effective security implementation.

The entire sector understands it has vulnerable interdependencies and, as a result, the FSSCC and FS/ISAC work closely with other critical infrastructure sectors, key software providers, and government leaders to increase regional coordination efforts. This initiative was prompted by a consensus that, beyond New York City, existing activities at the regional level did not adequately address the critical infrastructure protection concerns of financial institutions. As illustrated in our recommendation for metropolitan-area security coordination, the financial services model is applicable to other regions and other sectors.

Two examples of cooperative efforts to assist in preparing for and successfully addressing risks associated with catastrophic events illustrate this point: One is the industry's development, in conjunction with the Securities Industry Association, of a set of considerations for actions to be taken by individual financial institutions and the sector broadly at each of the DHS homeland security alert levels. The goal is to give institutions a step-by-step plan of action to use in response to change in the homeland security alert levels. The second is the successful work of the Treasury Department and a range of organizations in the Chicago area to establish ChicagoFIRST.¹² Begun in 2003, ChicagoFIRST is a coalition of banks, security exchanges, and clearinghouses that ensures emergency management personnel are available to assist crisis managers in protecting financial interests. ChicagoFIRST was created with the premise that, should a terrorist attack or other crisis occur, it is highly likely that it will be concentrated on one geographic area, rather than on a national level. This coalition secured a seat in Chicago's Joint Operations 911 Center, created secure credentials for personnel, defined evacuation procedures for financial personnel, and participated in tabletop exercises with state and federal agencies. Additionally, ChicagoFIRST produced a handbook, funded by the Treasury Department and coauthored by BITS, and the Boston Consulting Group, for other regions seeking to establish similar coalitions. At this writing, Miami banks have announced plans to create a similar coalition, FloridaFIRST.

When Hurricane Katrina struck, the financial services industry again tested its ability to respond effectively to a devastating situation. Executives had immediate access to coordinated information for making critical decisions as the disaster was occurring and in the hours and days that followed.

That information included communications directly from the Treasury and the Department of Homeland Security, such as impact assessments, updates on critical cash supplies, the status of FEMA's distribution of debit cards, talking points for call center representatives as they assisted customers, guidance from regulatory agencies, and important contacts for additional support. These actions kept confidence in financial markets stable.

REGULATION AND SECURITY

Financial institutions are heavily regulated and actively supervised by state and federal agencies. At the federal level, these include the Federal Reserve, Federal Deposit Insurance Corporation, Office of the Comptroller of Currency, Office of Thrift Supervision, National Credit Union Administration, and the Securities and Exchange Commission. Although the financial services industry might prefer less regulation, it also recognizes that some regulations provide predictability, stability, and a foundation for public trust.

Security requirements that result from regulation may increase the cost of doing business, but the financial services sector remains very profitable nonetheless. The security required by regulation is borne equally by all institutions of a similar type (credit unions, stock brokerage houses, and so forth), eliminating security costs as a liability-affecting competitive advantage. The success of the security regulation also depends on active auditing to ensure compliance. The auditing is conducted by third-party accounting firms and federal agencies. Identified weaknesses must be remediated as part of this process. The regulators are aware that, in addition to the physical security of banks, the sector's security depends upon the reliability of:

- ◆ key vendors to the sector (software, communications, and so forth);
- ◆ continuity of operations plans and redundant capabilities; and
- ◆ continuous vetting of employees with access to sensitive systems.

Federal and state regulators have stepped up their oversight of business continuity, information security, third-party service providers, and critical infrastructure protection. The financial exchanges have also added

requirements in these areas. As the industry works with leaders to institute best practices and implement the most effective disaster recovery strategies, we also are working diligently to comply with evolving regulations and ongoing examinations.

The Department of Homeland Security proposed a rule to establish procedures for the receipt, care, and storage of Critical Infrastructure Information voluntarily submitted to the federal government through the Department of Homeland Security. There is widespread concern in the industry with the scope and implementation of the procedures. For the rule to be effective, strong safeguards must be in place. It is imperative that the DHS commit to implementing robust controls to protect the employee and customer information submitted by financial institutions.

RECOMMENDATIONS

We can draw numerous lessons from the work of the financial services sector in response to the attacks of September 11, the August 2003 blackout, and most recently Hurricanes Katrina and Rita. The most important and obvious are that preparedness matters and using established risk management practices now will ensure economic viability in the future. An important part of being prepared is looking strategically and holistically at the nation's critical infrastructure and what can be done to enhance resiliency and reliability. Regardless of how well the financial institutions respond to regulations, they alone simply cannot address these problems. Their partners in other critical industry sectors—particularly the telecommunications, energy, and software industries—must also do their fair share to ensure the soundness of these vital economic contributors. Further, the risks for national security and economic soundness cannot be underestimated, and neither can the importance of our working together to address them.

6.1. DIVERSE AND RESILIENT COMMUNICATION CHANNELS ARE ESSENTIAL. Elements such as cell phones, wireless e-mail devices, land-line phones, and the Internet are required. However, both diversity and redundancy are needed within critical infrastructures to assure backup systems are operable and continuity of services is maintained. Closely

related to this is the importance of having accurate and timely information about the scope and cause of major events. For example, during the August 2003 blackout, the announcement that the problem was not the result of a terrorist event alleviated public concern and enhanced the orderly execution of business continuity processes. High-impact targets should explore installation of redundant communication networks to key security and response elements.

6.2. THE POWER GRID MUST BE CONSIDERED AMONG THE MOST VITAL OF CRITICAL INFRASTRUCTURES AND NEEDS INVESTMENT TO MAKE SURE IT WORKS ACROSS THE NATION. The cascading impact on the operation of financial services, access to fuel, availability of water, and sources of power for telephone services and Internet communications cannot be overstated.

6.3. RECOGNIZE THE INTERDEPENDENCIES AMONG CRITICAL INFRASTRUCTURE SECTORS. Those of greatest concern to us are the interdependencies among financial services, telecommunications, and energy sectors. The federal government should take action to enhance the diversity and resiliency of the telecommunications infrastructure and the nation's energy grids.

6.4. RECOGNIZE THE DEPENDENCY OF CRITICAL INFRASTRUCTURES ON SOFTWARE OPERATING SYSTEMS AND THE INTERNET. A clear understanding of the role of software operating systems within critical infrastructures needs to be explored, including ways of sharing responsibility and liability more equitably among stakeholders. The financial services sector has endorsed an agenda to improve cyber security, but, in addition to those recommendations, the financial services industry needs to improve the physical security of the cyber network nodes on which it relies to eliminate single points of failure.

6.5. AS HURRICANE KATRINA HAS POIGNANTLY ILLUSTRATED, ESTABLISHING IMPROVED COORDINATION PROCEDURES ACROSS ALL CRITICAL INFRASTRUCTURES AND WITH FEDERAL, STATE, AND LOCAL GOVERNMENT IS ESSENTIAL TO RAPID, COORDINATED, AND EFFECTIVE RESPONSE WHEN EVENTS OCCUR. To minimize the economic and social risks during a crisis, coordination in planning and response between the private sector and public emergency management must improve.



While the financial services sector has a long agenda of security improvements yet to be implemented, our national security overall would be greatly enhanced if other key sectors of our economy were as secure as our financial services infrastructure is already.

