

CYBER SECURITY FOR THE BANKING AND FINANCE SECTOR

VALERIE ABEND AND BRIAN PERETTI

Department of Treasury, Washington, District of Columbia

C WARREN AXLEROD

Bank of America, Charlotte, North Carolina

ANDREW BACH

NYSE Euronext, New York, New York

KEVIN BARRY, DON DONAHUE AND KEN WRIGHT

Depository Trust and Clearing Corporation, New York, New York

JOHN CARLSON

BITS, Washington, District of Columbia

**FRANK CASTELLUCCIO, DAN DEWAAL, DAVID ENGALDO AND GEORGE
HENDER**

Options Clearing Corporation, Chicago, Illinois

DAVID LAFALCE

The Clearing House, New York, New York

MARK MERKOW

American Express Company, New York, New York

WILLIAM NELSON

FS-ISAC, Dulles, Virginia

JOHN PANCHERY

Securities Industry Financial Market Association, New York, New York

DAN SCHUTZER

Financial Services Technology Consortium, New York, New York

DAVID SOLO

Corporate Technology Office, Citigroup Inc., New York, New York

JENNIFER L. BAYUK

LLC, New York, New York

Wiley Handbook of Science and Technology for Homeland Security, Edited by John G. Voeller
Copyright © 2008 John Wiley & Sons, Inc.

Abstract: The banking and finance sector requires secure, resilient, and reliable systems to ensure seamless operations and maintain public confidence in monetary systems. Many financial institutions are at the forefront of developing best practices and deploying advanced technologies to secure their systems and assets. More importantly, the sector serves as a model of the cooperation necessary to develop standards and best practices that benefit all sectors. This article identifies some of the important cyber security-related collaboration among the private and public sector organizations that make up the sector, and explores the culture that enables such cooperation.

Information security is an important concern for all institutions in the banking and finance sector. Financial institutions are persistently targeted by criminals and others with malicious intent. To address these problems, institutions across the sector worked collaboratively to improve inter- and intrasector communication and created private–public partnerships for information sharing and encouraging innovation. This article explores the foundations of cooperation and information sharing, including some of the major initiatives, associations, and challenges the sector faced as it worked to improve defenses against attack, enhance resiliency, and sustain public confidence in trusted banking relationships.

Keywords: information security; financial services

1 HISTORY OF COOPERATION

The US government and financial institutions have a long history of cooperation. The government recognized financial institutions as an integral part of the nation’s critical infrastructure. As such, financial institutions are highly regulated and constantly supervised by regulatory agencies to ensure that they are able to withstand the various and increasing threats they face.

Examples of cooperation between the public and private sector in the late 1990s include preparations for the Century Date Change or “Y2K”, *Preliminary Research and Development Roadmap for Protecting and Assuring Critical National Infrastructures* (July 1998) by the President’s Commission on Critical Infrastructure Protection (PCCIP) and the Critical Infrastructure Assurance Office (CIAO),¹ and Presidential Decision Directive (PDD) 63 on Critical Infrastructure Protection (CIP, May 1998). PDD 63 established the first governmental approach to protecting the nation’s critical infrastructures, assigning responsibility for protecting infrastructures in different economic segments to different governmental agencies, provided each responsible agency would appoint a private sector “Sector Coordinator” to work with the agency to pursue infrastructure protection in the sector, and encouraging the sharing of infrastructure protection information between government and private industry through the formation of information sharing and analysis centers (ISACs). It also supported research and development, outreach, and vulnerability assessment. PDD 63 described “A National Goal” as follows:

¹The *Preliminary Research and Development Roadmap for Protecting and Assuring Critical National Infrastructures* is available at http://cipp.gmu.edu/archive/190_PCCIPCIAORandDRoadmap_0798.pdf Other pertinent documents can be found in the CIP Digital Archive in the George Mason University School of Law Critical Infrastructure Protection Program website at <http://cipp.gmu.edu/clib/CIPDigitalArchive.php>.

“No later than the year 2000, the United States shall have achieved an initial operating capability and no later than five years from today [i.e. by May 22, 2003] *the United States shall have achieved and shall maintain the ability to protect the nation’s critical infrastructures form intentional acts that would significantly diminish the abilities of*

- the Federal Government to perform essential national security missions and to ensure the general public health and safety;
- state and local governments to maintain order and to deliver minimal essential public services;
- *the private sector to ensure the orderly functioning of the economy and the delivery of essential telecommunications, energy, financial and transportation services.*” [emphasis added]

Under PDD 63, the Department of the Treasury (“Treasury”) was assigned the responsibility for the banking and finance sector, and appointed Steve Katz, then Chief Information Security Officer for Citibank, as the first private sector “Sector Coordinator”.

In the following years, the US Congress focused on cyber security issues as it related to privacy protection. Two significant laws governing privacy and security protections were enacted in the 1990s, the Health Insurance Portability and Accountability Act of (1996) also known as (HIPAA) and the Financial Services Modernization Act of 1999,² also known as the Gramm–Leach–Bliley Act (GLBA) (1999).

HIPAA³ was enacted to restrict control of and access to patients’ information and GLBA includes a provision requiring financial institutions to safeguard personal information. In 2001, regulators finalized regulations requiring financial institutions to establish appropriate safeguards for the use, disclosure, privacy, and security of personal information, including Social Security Numbers (SSNs). The regulators applied strong enforcement tools to ensure that financial institutions complied with these security requirements. In addition, the Federal Financial Institutions Examination Council (FFIEC),⁴ issued several Information Technology booklets on topics including information security, business continuity planning (BCP), and outsourcing.⁵

In January 2000, the Clinton Administration released *Defending America’s Cyberspace: National Plan for Information Systems Protection, Version 1.0: An Invitation to a Dialogue*. This report urged the creation of public private partnerships to address cyber security issues

Shortly after the 9/11 attacks of September 11, 2001, the government and financial services industry responded. Executive Order (EO) 13228⁶ *Establishing the Office of Homeland Security (HLS) and the Homeland Security Council* created the present structure for the protection of the homeland and EO 13231⁷ *Critical Infrastructure Protection in the Information Age*, outlined, *inter alia*, the public partnerships context for the protection of the critical infrastructure. Private sector advisory councils were formed, including the Homeland Security Advisory Council(HSAC) (EO 13228) and

²Public Law No. 106–102.

³Public Law 104–191, 42 U.S.C. 1301 et seq.

⁴An interagency body with representation from the Board of Governors of the Federal Reserve System, Federal Deposit Insurance Corporation (FDIC), the National Credit Union Administration (NCUA), Office of the Comptroller of the Currency (OCC), and Office of Thrift Supervision (OTS).

⁵These Booklets are available at www.ffiec.gov/guides.htm.

⁶http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=2001_register&docid=fr10oc01-144.pdf.

⁷http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=2001_register&docid=fr18oc01-139.pdf.

the National Infrastructure Advisory Council (NIAC) (EO 13231). The Office of HLS, first headed by former Pennsylvania Governor Thomas Ridge, was formed. In addition, the President's Critical Infrastructure Protection Board (PCIPB), based on the Clinton administration's *Defending America's Cyberspace* plan, was established. The PCIPB coordinated an effort to draft a national infrastructure protection strategy that included contributions from both public and private participants. All participants were asked to comment on how this effort should evolve. In particular, the goal was to avoid legislation and regulation by means of proactive collaborative measures. Each of the critical sectors was directed to publish its own strategy.⁸

Several financial services industry organizations supported these efforts, including the Securities Industry Association (formerly SIA, now Securities Industry and Financial Markets Association [SIFMA]), BITS (the Financial Services Roundtable's technology and operations division), and the Financial Services Information Sharing and Analysis Center (FS-ISAC). This support was intended to foster closer working relationships between government and the finance sector.

The US financial regulators and the US Treasury Department were also looking at these issues. Following a series of organizational meetings in 2001, the US Treasury and financial regulators developed a process to coordinate the activities of federal and state financial services regulators by establishing the Financial and Banking Information Infrastructure Committee (FBIIC).⁹

The FBIIC, originally a standing committee of the PCIPB, but currently chartered under the President's Working Group on Financial Markets, is charged with improving coordination and communication among financial regulators, enhancing the resiliency of the financial sector, and promoting the public-private partnership. Treasury's Assistant Secretary for Financial Institutions chairs the committee.

In fulfilling its mission, the FBIIC set out to:

- identify critical infrastructure assets, their locations, potential vulnerabilities, and prioritize their importance to the financial system of the US;
- establish secure communications capability among the financial regulators and protocols for communicating during an emergency; and
- ensure sufficient staff at each member agency with appropriate security clearances to handle classified information and to coordinate in the event of an emergency.

Working with appropriate members of financial institution regulatory agencies, the FBIIC has accomplished the following:

- provided key federal and state financial regulators with secure telecommunications equipment for use in a crisis, and we adding a capacity for encrypted e-mail;
- written emergency communications procedures allowing communication between financial regulators and Federal, state, and local stakeholders;
- worked to systematically identify critical financial infrastructures, assess vulnerabilities within the critical financial infrastructure, address vulnerabilities, and evaluate progress; and

⁸The entire list of sector plans, as well as copies of the plans, are available at the website of the Partnership for Critical Infrastructure Security (PCIS) at www.pcis.org.

⁹Membership information can be found at www.fbiic.gov.

- identified the infrastructure that is critical to the retail payments system, the insurance industry, and the housing finance industry.

On May 10, 2002, key leaders from the financial services industry, with the encouragement of the Treasury, established the Financial Services Sector Coordinating Council (FSSCC).¹⁰ Rhonda MacLean, then Chief Information Security Officer at Bank of America Corporation, was appointed the second Sector Coordinator for Financial Services by Treasury, and served as the founding Chairman of the FSSCC. The banking and finance sector published its first version of the sector's critical infrastructure protection plan in May 2002. The "National Strategy for Critical Infrastructure Protection" was jointly drafted by several associations including BITS, SIA, FS-ISAC, AbA, and in consultation with the financial regulators.¹¹

Members of the FSSCC and FBIIC meet three times a year for discussions and briefings.

On September 18, 2002, the Bush administration released a draft of *The National Strategy to Secure Cyberspace*. The *National Strategy* outlined the "preferred" means of interaction between the public and private sectors. After incorporating comments, the Bush administration released the final *National Strategy to Secure Cyberspace* in February 2003.¹² On March 1, 2003, the Department of Homeland Security (DHS) was formally established and many of the responsibilities of the PCIPB were transferred to DHS.

In September 2002, several regulatory agencies released a draft paper outlining more stringent BCP requirements for certain types of large financial institutions. The *Draft Interagency White Paper on Sound Practices to Strengthen the Resilience of the US Financial System* was released for public comment by the Federal Reserve Board (FRB), Office of the Comptroller of the Currency (OCC), Securities and Exchange Commission (SEC), and the New York State Banking Department. Several financial institutions and associations submitted detailed comment letters on the proposal and objected to several onerous proposed requirements. In April 2003, three of the original agencies (the FRB, OCC, and SEC) released the final *Sound Practices White Paper* after considering 90 comment letters from industry participants.¹³ The revised final paper did not insist on a minimum distance between primary and backup sites (e.g., 300 mile minimum distance between primary and backup sites). However, it does require that institutions have staff, located outside their primary sites, which can conduct business if those at the primary site cannot get to the backup facilities. This became a good precedent for how meaningful, respectful discussion can lead to a proposal that meets requirements but is not overly burdensome on industry members.

In 2003, the President released the *National Strategy to Secure Cyberspace* and *National Strategy for Physical Protection of Critical Infrastructures and Key Assets*. These documents called for Treasury, as the lead agency for the banking and finance sector, to develop a research and development agenda for the sector. Treasury, working

¹⁰Details about the FSSCC and its activities can be found at the FSSCC website at www.fsscc.org.

¹¹A 2004 update of this strategy and other publications about the FSSCC's activities can be found at the FSSCC website.

¹²*The National Strategy to Secure Cyberspace*, The White House, February 2003, is available at www.whitehouse.gov/pcipb/cyberspace_strategy.pdf. This document implements a component of *The National Strategy for Homeland Security* and is complemented by *The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets*, which are available at www.whitehouse.gov/pcipb/physical_strategy.pdf.

¹³The Interagency Paper is available at www.sec.gov/news/studies/34-47638.htm.

with the FBIIC and the FSSCC, published an agenda for the sector entitled “Closing the Gap”. The driving force behind the document was a desire to identify key areas where additional research dollars could be spent to make the sector more secure. This document was socialized among Federal departments and agencies, academics, and financial services participants.

On March 7 and 8, 2005, Treasury, in conjunction with the National Science Foundation (NSF), hosted a workshop entitled “Resilient Financial Information Systems”. Participants from academia and the public and private sectors worked to discuss and identify research priorities to advance the resilience of the financial sector and protect the nation’s critical financial infrastructure. As the issue of research and development (R&D) for the financial services sector matured, the FSSCC developed a working group to focus specifically on the issue for R&D and to coordinate its activities with respect to critical infrastructure and key resources (CI/KR) R&D. At Treasury’s request, the FSSCC joined DHS in a May 2005 workshop focused on R&D priorities.

DHS published an updated version of the National Infrastructure Protection Plan (NIPP) in 2005. The role of the sector-specific agencies in coordinating the activities of the sector was again reaffirmed in the document. As DHS was finalizing the NIPP R&D plans and programs, the FSSCC formed an R&D Committee to focus on those plans and programs that would provide the most significant benefits with respect to the specific CI/KR requirements of the financial services industry. In May 2006, this committee issued a list of priority research projects. The FSSCC Research and Development Committee Research Challenges and the FSSCC Research and Development Research Agenda were issued to assist researchers in focussing research on top concerns.¹⁴ In February 2008, the FSSCC R&D Committee began to “beta test” the Subject Matter Advisory Response Team (SMART) program. The SMART program assists research and development organizations working on Critical Infrastructure Protection Projects by providing subject matter expertise for financial institutions necessary to facilitate their R&D endeavors.

2 ORGANIZATIONAL ROLES

2.1 FSSCC

The Financial Services Sector Coordinating Council (FSSCC) for critical infrastructure protection and homeland security (CIP/HLS) is a group of more than 30 private sector firms and financial trade associations that works to help reinforce the financial services sector’s resilience against terrorist attacks and other threats to the nation’s financial infrastructure. Formed in 2002, FSSCC works with Treasury, which has direct responsibility for infrastructure protection and HLS efforts for the financial services sector.

The mission of the FSSCC is to foster and facilitate the coordination of financial services sector-wide voluntary activities and initiatives designed to improve CIP/HLS. Its objectives are to:

- provide broad industry representation for CIP/HLS and related matters for the financial services sector and for voluntary sector-wide partnership efforts;
- foster and promote coordination and cooperation among participating sector constituencies on CIP/HLS related activities and initiatives;

¹⁴Both of these documents are available at www.fsscc.org.

- identify voluntary efforts where improvements in coordination can foster sector preparedness for CIP/HLS;
- establish and promote broad sector activities and initiatives that improve CIP/HLS;
- identify barriers and recommend initiatives to improve sector-wide voluntary CIP/HLS information and knowledge sharing and the timely dissemination processes for critical information sharing among all sector constituencies; and
- improve sector awareness of CIP/HLS issues, available information, sector activities/initiatives, and opportunities for improved coordination.

As described above, the FSSCC is the private side of the public–private partnership which supports the National Infrastructure Protection Plan (NIPP). The other organizations listed in this section are all members of the FSSCC. Each organization has strengths in different areas, allowing the FSSCC to coordinate efforts of various members in support of overall infrastructure protection goals. Since the FSSCC was established, it has been chaired by distinguished and prominent members of the financial community Rhonda MacLean of Bank of America from 2002–2004, Donald Donahue of The Depository Trust and Clearing Corporation from 2004 through 2006 and George S. Hender of The Options Clearing Corporation from 2006 to 2008, and Shawn Johnson of State Street Global Advisors in 2008.

2.2 FSSCC Member Organizations

All FSSCC member organizations have contributed to industry goals for CIP. The organizations described below have provided the most direct focus on collaboration with respect to cyber security issues in the Banking and Finance Sector.

2.2.1 BITS In 1996, members of Bankers Roundtable (now The Financial Services Roundtable) created BITS in order to respond to significant technological changes facing the banking industry. BITS initially focused on changes in electronic commerce and the payments system, but evolved over time to focus on new threats that emerged in the areas of Internet security, fraud reduction, and CIP. Before 9/11, BITS helped to create the FS-ISAC. After 9/11, BITS helped to create the FSSCC and ChicagoFIRST.¹⁵

In 2001, BITS established the BITS Crisis Management Coordination Working Group (CMC-WG). This working group implemented The BITS and Financial Services Roundtable Crisis Communicator, a high-speed communications programs, that allowed the organization to connect all the key players—member CEOs and government and other business leaders—who might need to convene and determine how to address a crisis. The *BITS and Financial Services Roundtable (FSR) Crisis Management Process: Members' Manual of Procedures* was developed to provide BITS' members with the ability to communicate and coordinate with each other, government agencies, and other sectors in order to implement the emergency response and recovery process for the financial services sector.

One of the greatest lessons learned from 9/11 was the extent of the financial services sector's interdependencies and reliance on other critical sectors, specifically telecommunications and power. With the help of the Board of Governors of the Federal Reserve System, notably Steve Malphrus, BITS convened a conference in New York City in

¹⁵ChicagoFIRST is a nonprofit association dedicated to addressing HLS and emergency management issues affecting financial institutions and requiring a coordinated response.

July 2002. The conference focused on ways to get tangible progress from other critical infrastructure sectors toward the goal of cooperation between government and the private sector.

One tool that resulted from the BITS Telecommunications Working Group efforts is the *BITS Guide to Business—Critical Telecommunications Services*. Completed in 2004¹⁶, the Guide is based on extensive work by BITS members, participation by major telecommunications companies, and involvement by the National Communications System (NCS) and the President’s National Security Telecommunications Advisory Council (NSTAC). The Guide is a comprehensive tool used by BITS’ member institutions to better understand the risks of telecommunications interdependencies and achieve greater resiliency.

2.2.2 ChicagoFIRST Another clear lesson from 9/11 was the stunning impact an event could have on critical financial services operations that are heavily located in one regional area. Louis Rosenthal, ABN AMRO, and Ro Kumar, The Options Clearing Corporation, saw the potential risks in the Chicago area and energized their peers and a set of partners. BITS facilitated the process of forming the regional coalition. In 2003–04 the US Treasury Department founded an evaluation and guide for establishing regional coalition through the Boston Consulting Group and BITS. ChicagoFIRST, the result of these efforts, is a free-standing nonprofit organization that provides robust coordination services to maintain the resilience of the critical financial services that reside in the area. It continues to serve as a model for others, including FloridaFIRST and other regional coalitions.¹⁷

2.2.3 Financial Services Information Sharing and Analysis Center (FS-ISAC) The FS-ISAC was conceived at a meeting of Financial Industry leaders with the Treasury at the White House Conference Center in March 1999. An Information Sharing Working Group was established. The financial services industry members participating in the original Information Sharing Working Group appointed a Board of Managers, who formed FS-ISAC limited liability corporation (LLC). It was officially launched by US Treasury Secretary Lawrence A. Summers at a ceremony in the Treasury building on October 1, 1999, as a means of meeting the finance sector’s information-sharing obligation under PDD 63 on CIP.

On December 9, 2003, the Treasury announced that it would purchase \$2 million in services from the FS-ISAC. Treasury’s contract with the FS-ISAC resulted in a new, next-generation FS-ISAC that is intended to benefit the Treasury, other financial regulators, and the private sector. In the press release, the Treasury indicated the purposes for the funding were as follows¹⁸

- Transform the FS-ISAC from a technology platform that serves approximately 80 financial institutions to one that serves the entire 30,000 institution financial sector, including banks, credit unions, securities firms, insurance companies, commodity futures merchants, exchanges, and others.

¹⁶The BITS Telecommunications Working Group, led by John DiNuzzo (formerly of FleetBoston/Bank of America Corporation) was a subgroup of the BITS CMC-WG.

¹⁷Improving Business Continuity in the Financial Services Sector: A Model for Starting Regional Coalitions (US Treasury: November, 2004). http://www.treas.gov/press/releases/reports/chicagofirst_handbook.pdf

¹⁸http://www.ustreas.gov/press/releases/reports/factsheet_js1048.pdf.

- Provide a secure, confidential forum for financial institutions to share information among each other as they respond in real time to particular threats.
- Add information about physical threats to the cyber threat information that the FS-ISAC currently disseminates.
- Include an advance notification service that will notify member financial institutions of threats. The primary means of notification will be by Internet. If, however, Internet traffic is disrupted, the notification will be by other means, including telephone calls and faxes.
- Include over 16 quantitative measures of the FS-ISAC's effectiveness that will enable the leadership of the FS-ISAC and Treasury to assess both the FS-ISAC's performance and the aggregate state of information sharing within the industry in response to particular threats.

The FS-ISAC was able to arrange with a managed security service provider to fund the initial development and implementation of the FS-ISAC systems and networks in return for the right to reuse the technology developed. The FS-ISAC thus succeeded in meeting its original goal of becoming a viable means for the banking and finance sector to share information about security threats, vulnerabilities, incidents, and remedies. E-mail alerts and notifications sent by the FS-ISAC give financial firms advanced notice of threats, vulnerabilities, and events so that they can proactively protect themselves. The FS-ISAC also hosts an information-sharing website, conference calls, and conferences that allow its members more interactive sharing opportunities.

In 2006, the FS-ISAC established a Survey Review Committee to provide oversight of the process of member-submitted surveys of the FS-ISAC membership. The FS-ISAC survey process allows for one live poll at a time to ensure maximum participation. The primary contact at each member organization is asked to complete each survey or route it to the appropriate area within their company to have it answered by the most qualified individual. Surveys conducted in 2007 included *Employee Access to HR Information*, *Data Transfer Methods*, and *Information Security Program Organization*. Once the survey is completed, a Poll Results Report is created that includes a brief summary and the final poll results. Using the survey tool link provided, members can also conduct their own detailed analysis of survey results to meet their unique needs.

Through the personal involvement of members of the FS-ISAC's Board of Managers and the FS-ISAC membership at large, the reach of the FS-ISAC members¹⁹ quickly spread well beyond the original mandate. Early on, board members were involved in efforts such as

- participating, through the FSSCC, in drafting the finance sector's segment of Version 2.0 of the NIPP;
- assisting in, and being supportive of, the establishment of the BITS laboratory for testing and certifying security software relevant to financial services institutions;
- working with Treasury to develop an outreach and education program to increase awareness of sector security threats, vulnerabilities, and best practices, and to indicate how the FS-ISAC might assist them in these areas;
- briefing Federal agencies as to the workings of the FS-ISAC; and

¹⁹The Board of Managers and members of the FS-ISAC are not restricted from other industry activities beyond the work of the FS-ISAC.

- testifying before congressional committees and otherwise representing the views of the banking and finance sector on cyber security and CIP.

The FS-ISAC has been a model for a number of other ISACs in critical US sectors, such as transportation, energy and information technology, as well as ISACs in foreign countries (e.g. Canada) and in individual corporate organizations (e.g. the Worldwide ISAC). Its October 2007 biannual conference was recently coordinated in conjunction with the CIP Congress, carrying the theme “When Failure is Not an Option” and was accordingly attended by members of other ISACs.

2.2.4 FSTC The Financial Services Technology Consortium (FSTC) was established in 1993 at the dawn of the commercialization of the Internet. FSTC is a nonprofit organization with members from the financial services industry (financial services providers and vendors), government agencies, and academia, who collaborate on projects to explore and solve strategic business–technology issues through concept validation, prototype and piloting, and development of standards. Its mission is to harness technology advances and innovative thinking to help solve the problems of the financial services industry.

Early projects dealt with paper check imaging, the convergence of the payments products, and securing electronic banking, commerce, and payments over the Internet. These projects helped spur the growth of electronic commerce and paved the way for Check 21 and the electronification of the paper check through the development of important new standards and industry utilities and collaborations.

After September 11, FSTC’s focus expanded to include addressing business continuity issues in addition to security, fraud management, and payments, leading to a partnership with Carnegie Mellon that developed a Resiliency Framework. FSTC also initiated a focus on enterprise architecture aimed at helping financial services firms to streamline and consolidate their siloed systems and processes, enabling the reduction of redundant processes and systems, to provide a more efficient and flexible organization, able to more rapidly and easily accommodate new products, services, and processes needed to meet new business opportunities and threats.

FSTC thrives when the knowledge of members comes together through the formation of initiatives and projects that will better the industry as a whole. FSTC projects are its core activity and one of the key benefits of FSTC membership.

2.2.5 SIFMA SIFMA provides a forum for securities firms, exchanges, industry utilities, and regulators to share knowledge, plans, and information. It is responsible for developing and promoting industry-specific practice guidelines, for providing liaison between the securities industry and regulators and legislators, and for coordinating industry-wide initiatives. SIFMA has standing committees to coordinate industry-wide initiatives for various types of securities industry trading and operations activities.

The SIFMA BCP Committee was established as the SIA BCP in November 2001 to address and coordinate business continuity issues for the securities industry. In conjunction with the BCP Committee mission, SIFMA (and its predecessors, the SIA and the Bond Markets Association) has led an extensive on-going industry-wide business continuity testing initiative since 2002. The effort allows the industry as a whole to verify and demonstrate the resilience of the securities markets and to provide individual firms with opportunities to test their procedures with other industry participants in a way they could not do on their own. Industry tests include tabletop exercises, connectivity tests, communications tests, participation in national disaster recovery tests, and pandemic

flu exercises. SIFMA in conjunction with the BCP Committee operates the Securities Industry Emergency Command Center that functions as the industry's central point of emergency communications and coordination during significant emergencies.

Initial testing efforts in 2002, 2003, and 2004 involved basic connectivity tests between individual firms and exchanges. Much more robust business continuity tests were conducted in 2005 and 2006. Over 250 firms, exchanges and industry utilities participated in these tests, which involved transmission of dummy transactions from firms' and exchanges' backup sites using backup communications links. The industry demonstrated a 95% pass rate on these tests. SIFMA also coordinates securities industry participation in the national TopOff emergency exercises and focuses heavily on planning for a potential flu pandemic and on conducting pandemic planning exercises.

SIFMA's Information Security Subcommittee, which was established in 2003, addresses and coordinates information security issues from an industry perspective and facilitates information sharing among SIFMA member firms. The Subcommittee provides comments to regulatory authorities on proposed information security rules and regulations and develops industry initiatives. The Subcommittee has focused on a variety of issues including developing guidance on the design and testing of Sarbanes Oxley controls, working with legislators on proposed Security Breach Legislation, tracking and assessing Microsoft security releases, and establishing guidance on effective means of dealing with phishing attempts.

In 2007, SIFMA formed the Information Risk Advisory Council to provide advice to SIFMA's Technology, Information Security, BCP, and Privacy Committees. The Council identifies issues of significant importance to securities firms and works with SIFMA Committee to integrate these into the committees' annual goals.

3 SAMPLE SIGNIFICANT EVENTS

Although cyber security-related events are a daily occurrence in the financial industry, some events are more significant than the others with respect to collaborative information sharing. The events listed below were significant in that the collaboration that occurred during the event served to strengthen the bonds of communication between public and private sector CIP organizations.

3.1 Russian Hacker Case

In June 1994, a Russian crime ring managed to get inside the Citibank computer system and transfer \$140,000 from the Philippine National Bank to a bank in Finland. The bank in the Philippines called to complain that the transaction had not been authorized. Citibank realized something was amiss and set up a special team to start looking into transactions of similar circumstance. However, it was not given that the unauthorized transfer was the first discovery of a chain of illegal activity. By the middle of July, the team identified a similar transfer had taken place and yet a third by the end of the month. By this time, Citibank had called in the Federal Bureau of Investigation (FBI) and the investigation was in full swing. Transactions were being illegally transferred from cities as far away as Djakarta and Buenos Aries to banks in San Francisco and Israel. In total, fraudulent transactions amounted to more than \$3 million; though in the end, the gang of thieves managed to abscond with only \$400,000.

The system breached was called the Citibank Cash Management system. This system allowed corporate customers to transfer money automatically from their accounts to whoever they are paying. And it handled approximately 100,000 transactions a day, totaling \$500 billion. The Citibank system relied on static passwords, which they intend for users to memorize. The passwords remain the same each time a user enters the system, and although they are encrypted, the crime ring was somehow able to get a password and identification numbers of some of these corporate customers. The investigation team realized that the passwords traversed through many network links that were not necessarily fully owned and operated by the bank, but many were leased from telecommunication companies in various countries which provided the bank with network links between its offices. The question the investigators faced was did the perpetrator have an insider in Citibank or was he able to get them using conventional “network-sniffing” software.

On August 5, a fraudster transferred \$218,000 from a Citibank account in Djakarta and another \$304,000 from a bank in Argentina to Bank of America accounts in San Francisco that had been set up by a Russian couple. They would go to the bank after the money was transferred and attempt to withdraw it. At that point, investigators identified the perpetrators. They were kept under observation by both the public and private sector through October, transferring money from and to more accounts.

The idea of computer control of funds was new to the media at that time. It was a new idea to reporters that a person could be sitting at a computer in Russia in the middle of the night keying in passwords and watching money move across a screen. The Internet was still young at the time and largely unused commercially. The transfers were done through a proprietary network managed by Citibank. But, like the Internet, these proprietary networks cross over other proprietary networks and it is at these points that passwords become most vulnerable. Yet cooperation between the bank investigators, telecommunications administrators, and law enforcement led eventually to Vladimir Levin, a young Russian hacker. He was trapped through a traced telecommunications line performing a fraudulent transaction and was imprisoned. In the course of the investigation, several people were arrested (including half a dozen Russian citizens, which this story is known as the “Russian Hacker Case”). Immediately after, Citibank ended the use of static passwords over its Funds Transfer networks and started issuing One Time Password tokens to customers using those networks (these tokens were a form of two factor authentication from a small company named RSA from its founders, Rivest, Shamir, and Adelman, then infrequently encountered).

3.2 Slammer Worm

On January 23, 2003, a structured query language (SQL) injection dubbed the “slammer worm” started to infect rapidly through computer systems throughout the world. Although a patch was released for the vulnerability, many organizations had not installed it. As a result, the worm spread very quickly, infecting, by one account, 75,000 victims within 10 min after its release.

Although financial institutions were not greatly affected by the worm, Treasury, in coordination with the FBIIC and FSSCC, convened a meeting on February 25, 2003, to discuss issues related to the worm. In addition to members of the FBIIC and FSSCC, several private sector groups attended, including Microsoft and electronic data system (EDS). At the meeting, communications protocols were developed to aid in the sharing of information in the event of another incident. The protocols were exercised during several other virus/worm attacks, including SoBig.F and BugBear.b.

TABLE 1 Publications and Events

| Date | Name of Publication/Event | Comments |
|---------------|------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| February 1996 | CIWG (Critical Infrastructure Working Group) Report | Suggested establishing PCCIP (President's Commission on Critical Infrastructure Protection) for the longer-term view and the IPTF (Infrastructure Protection Task Force) for coordination of then existing infrastructure protection efforts. |
| July 1996 | EO (Executive Order) 13010 | Formed PCCIP, IPTF and CIAO (Critical Infrastructure Assurance Office) Available at www.fas.org/irp/offdocs/eo13010.htm |
| October 1997 | Critical Foundations: Protecting America's Infrastructures | Report issued by PCCIP suggesting a strategy incorporating research and development, information sharing, education, and awareness |
| May 1998 | PDD-63 (Presidential Decision Directive Number 63) for Critical Infrastructure Protection | By May 2003: the Federal Government to perform essential national security missions and to ensure the general public health and safety State and local governments to maintain order and to deliver minimum essential public services The private sector to ensure the orderly functioning of the economy and the delivery of essential telecommunications, energy, financial, and transportation services. |
| July 1998 | Preliminary Research and Development Roadmap for Protecting and Assuring Critical National Infrastructures | Report issued by PCCIP and CIAO as a follow-up of <i>Critical Foundations: Protecting America's Infrastructures</i> . Section 2.1 addresses the Banking and Finance sector |
| October 1999 | Official launch of the FS-ISAC (Financial Services Information Sharing and Analysis Center) | Launched by US Treasury Secretary Laurence P. Summers—available at www.fsisac.com |
| January 2000 | Defending America's Cyberspace: National Plan for Information Systems Protection, Version 1: An Invitation to a Dialog | This report urged the creation of public private partnerships to address cyber security issues |
| January 2001 | Report of the President of the United States on the Status of Federal Critical Infrastructure Protection Activities | Available at www.fas.org |

TABLE 1 (Continued)

| Date | Name of Publication/Event | Comments |
|---------------|-------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| March 2002 | Banking and Finance Sector: The National Strategy for Critical Infrastructure Protection | Available at www.pcis.org |
| May 2002 | Banking and Finance Sector National Strategy for Critical Infrastructure Assurance | Available at www.pcis.org |
| July 2002 | National Strategy for Homeland Security | Available at www.whitehouse.gov/homeland/book/ nat_strat_hls.pdf |
| February 2003 | The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets | Available at www.whitehouse.gov/pcipb/physical. html |
| February 2003 | The National Strategy to Secure Cyberspace | Available at http://www.whitehouse.gov/pcipb/ |
| March 2003 | FFIEC IT Examination Handbook: Business Continuity Planning | Available at www.ffiec.com |
| 2003 | PCIS Industry Compendium to the National Strategy to Secure Cyberspace | Analysis of plans and summary of commonalities. Available at www.pcis.org |
| July 2003 | Risk Management Principles for Electronic Banking, Basel Committee on Banking Supervision, Bank for International Settlements | Available at www.bis.org/publ/bcbs98.pdf |
| December 2003 | Homeland Security Presidential Directive (HSPD)—7 on Critical Infrastructure Identification, Prioritization, and Protection | Covers policy, roles and responsibilities of Secretary of Homeland Security, other offices, and so on, coordination with the private sector. Note: Consistent with Homeland Security Act of 2002, produce “National Plan for Critical Infrastructure and Key Resources Protection” within one year, that is, by December 2004. www.whitehouse.gov/news/releases/ 2003/12/print/20031217-5.html |
| May 2004 | Homeland Security Strategy for Critical Infrastructure Protection in the Financial Services Sector: Version 2 | Objectives of Financial Services Strategy: Identifying and reducing vulnerabilities in the financial services infrastructure to such attacks Ensuring the resiliency of the nation’s financial services infrastructure to minimize the damage and expedite the recovery from attacks that do occur, and |

TABLE 1 (Continued)

| Date | Name of Publication/Event | Comments |
|---------------|-----------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| February 2005 | National Infrastructure Protection Plan (Interim) | Promoting public trust and confidence in the financial services sector's ability to withstand and recover from attacks that do occur. Available at www.fsscc.org Superseded by June 2006 NIPP http://cipp.gmu.edu/archive/Interim NIPP Feb 05.pdf |
| 2005 | FFIEC IT Examination Handbook: Information Security | Available at www.ffiec.com |
| April 2003 | Interagency Sound Practices to Strengthen the Resilience of the US Financial System | Available at www.sec.gov/news/studies/34-47638.htm |
| April 2006 | FSSCC Research Challenges Booklet | Available at www.fsscc.org |
| June 2006 | National Infrastructure Protection Plan | Available at www.dhs.gov |
| October 2006 | FSSCC R & D Agenda | Available at www.fsscc.org |
| December 2006 | FSSCC Annual Report | FSSCC published the Banking and Finance Sector-Specific Plan as their annual report. Available at www.fsscc.org |
| May 2007 | Sector-Specific Plan: Banking and Finance Sector for Critical Infrastructure Protection | http://www.dhs.gov/xlibrary/assets/nipp-ssp-banking.pdf |
| 2005 (–2007) | Protecting the US Critical Infrastructure: 2004 (–2006) in Review | Annual reports, expected to continue, available at www.fsscc.org |

3.3 2003 Power Outage

At approximately 4:11 pm Eastern Daylight Time (EDT) on August 14, 2003, a power outage affected a large portion of the Northeastern United States, roughly from Detroit to New York City. Although there was minimal disruption to delivery of financial services in the affected area, the incident did expose a greater need to continue to examine the backup systems institutions. For example, the American Stock Exchange had relied upon steam power to cool their trading floor. Upon reaching out to the SEC and the Treasury, a backup steam generator was located and the exchange was able to open and close on Friday, August 15, 2003.²⁰ Many lessons learned from that set of events. One lesson led to the *BITS Guide to Business—Critical Power*, developed in cooperation with the Critical Power Coalition and Power Management Concepts, and published in 2006. It provides financial institutions with industry business practices for understanding, evaluating, and managing the associated risks, when the predicted reliability and availability of

²⁰The report, *Impact of the Recent Power Blackout and Hurricane Isabel on the Financial Services Sector*, can be found at <http://www.treas.gov/offices/domestic-finance/financial-institution/cip>.

the electrical system are disrupted—and it outlines ways by which financial institutions can enhance reliability and ensure uninterrupted backup power.

The following table, Table 1 describes a series of publications and events related to information sharing and coordination within the finance and banking sectors.

3.4 Pandemic Planning

In September and October 2007, SIFMA, in partnership with the FSSCC, the FBIIC, and the Treasury, conducted a multiweek pandemic flu exercise for the full financial services sector. This was the largest most ambitious financial services exercise to date that addressed business process recovery as a sector in communication with its sector-specific agency. The exercise offered a realistic simulation of the spread of a pandemic wave in the United States. It was designed to identify how a pandemic could affect the financial markets and to provide participants with an opportunity to examine their pandemic business recovery plans under a demanding scenario. Over 2700 financial services organizations participated.

3.5 Operation Firewall

On October 28, 2004, the US Department of Justice, in coordination with the United States Secret Service (USSS), executed over 28 search and arrest warrants in connect with Operation Firewall,²¹ an undercover investigation designed to stop the flow of stolen credit card numbers and other personal information. This operation lured criminals into a false sense of security by creating a fake website for buying and selling purloined credit card information. The main target was a group that called itself Shadowcrew, whose sole purpose was to defraud the financial services sector.

The operation, which lasted over an 18 month period, ended with the seizure of over 100 computers and the arrest of 28 individuals—21 in the United States and seven in Europe and Russia. Through the cooperation of several major financial services sector entities, the underground “carding” scene was dealt a major blow from which it is still attempting to recover.

4 FUTURE CHALLENGES

The examples above demonstrate high levels of collaboration among dedicated individuals representatives financial institutions, associations, and government agencies. For this collaboration to continue, it will require proactive engagement, open communications, and trust. The industry needs to cooperatively work with the respective agencies to develop rules and regulations that best meet the requirements of government while maintaining a strong finance sector and not overburdening financial institutions.

Since 9/11, government has proven its willingness to reach out and ensure the consensus of the financial community in its efforts to strengthen the infrastructure. It has also demonstrated increased trust on the part of the private side of the financial sector of government’s intent and a willingness to work with the various agencies, and to persuade others that cooperation is ultimately the best approach where each side can achieve its goals.

²¹<http://www.secretservice.gov/press/pub2304.pdf>.

FURTHER READING

- The FSSCC Research and Development Committee. (2006). *The FSSCC Research and Development Committee Research Challenges*, April 2006, <http://www.fsscc.org>.
- The FSSCC Research and Development Committee. (2006). *The FSSCC Research and Development Committee Research Agenda*, October 2006, <http://www.fsscc.org>.

CROSS-REFERENCES

- Homeland Security and Terrorism: Impact of World Events
- Homeland Security and Terrorism: The First Responder Perspective
- Infrastructure Interdependencies
- Computer Emergency Response Teams (CERTS)
- Survivability, Recovery and Reconstitution
- Red Teaming
- Critical Infrastructure Protection Decision Making
- Understanding the Implications of Critical Infrastructure Interdependencies
- National Infrastructure Protection Plan (NIPP)