The Critical Infrastructure Protection Program March 2006 / Volume 4, No. 9

THE CIP REPORT

Newsletter Editorial Staff

Editors

Jessica Milloy

Jeanne Geers

Staff Writers

Amy Cobb

Randy Jackson

Colleen Hardy

Maeve Dion

JMU Coordinators

John Noftsinger

Ken Newbold

Publishing

Zeichner Risk Analytics

Contact: cipp01@gmu.edu
703.993.4840

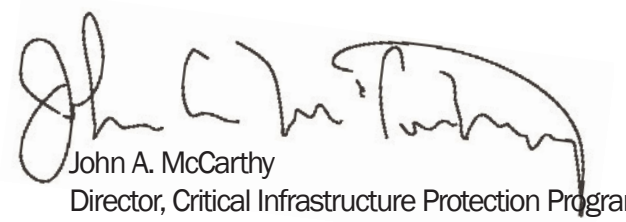
If you would like to subscribe to *The CIP Report* please click here. Visit us online for this and other issues at http://cipp.gmu.edu

GEORGE MASON UNIVERSITY
School of Law
CRITICAL INFRASTRUCTURE PROTECTION PROGRAM

This month's issue of *The CIP Report* features a highlight of the Banking and Finance Sector. Industry and government officials in this sector have made great strides over the last several years in the area of critical infrastructure protection. Many of the efforts required for protecting the nation's banking and finance infrastructure may have come more easily to this sector due to the fact that it has been carefully regulated since the Banking Act of 1933. Financial institutions have been held accountable for their stability through a rigorous bank examination routine for several decades.

Like all sectors, the advance of technology brought massive changes to the industry, and the sector has been forced to manage an array of unprecedented risks. Since the formation of the Finance Sector Information Sharing and Analysis Center in 1999 to prepare for Y2K, the sector at large has matured into an organized body. Due to the work of several innovative leaders and organizations, the sector enjoys extensive information sharing, open cross-sector and cross-industry communications, and advanced coordination for disaster preparedness planning. The key words for this sector's CIP efforts are business continuity and resilience.

In this month's issue, we take a look back to the financial community's response to Hurricane Katrina and a look ahead to the threat posed by an outbreak of 'avian flu' and the recommendations made by the Financial Services Coordinating Council. In addition to these pieces, we are also pleased to feature an interview with Catherine Allen, the CEO of BITS, a non-profit, CEO-driven financial services industry consortium comprised of 100 of the largest U.S. financial institutions. We also highlight ChicagoFIRST, a coalition dedicated to enhancing the resiliency of the financial community in the Chicago Metropolitan region, and the impact this model has had on the National Capital Region's similar efforts. Our goal is to present to our readers with a taste of the extensive coordination going on in a sector whose CIP efforts and accomplishments to date are impressive to say the least.



John A. McCarthy
Director, Critical Infrastructure Protection Program
George Mason University, School of Law

Finance Sector at Forefront of Resiliency, Business Continuity Planning

In a recent discussion with *The CIP Report*, Catherine A. Allen, CEO of BITS, laid out the progress that the financial sector has made over the last four and a half years in preparing for wide-scale disasters and disruptions. Although 9/11 was the impetus for sector coordination of business continuity and resiliency planning, the sector's efforts have been to prepare for any kind of event, whether natural or terrorist, physical or cyber.

Following 9/11, BITS initially led an effort to create best practices across the entire industry. Because of regulatory mandates, individual institutions had their own business continuity plans in place, however, there had not been a cross-industry exchange of best practices. The terrorist attacks underscored the need to address interdependencies as well, so BITS' focus has been to look both cross-industry and cross-sector to develop processes that will ensure communications and improve coordination during a disaster. One of the first steps was understanding the threats, so BITS launched a forum of experts on threat related topics, and met with military and government officials to understand and identify threat mitigation processes that could be adopted by industry.

One of the first documents developed for the sector's resiliency planning came after the Department of Homeland Security (DHS) launched its threat category system. BITS and the Securities Industry Association (SIA) responded to this new system by developing guidelines for what the financial sector should do for each threat level, using knowledge that it had gained from its network of experts. This document was the basis for a document developed by ASIS, a security organization, that serves as the official DHS recommendation for all sectors in responding to each threat level.

"There are numerous lessons we can draw from 9/11, the August 2003 blackout, and most recently, Hurricanes Katrina and Rita. The most important and obvious is to be prepared as well as resilient. An important part of being prepared is looking strategically and holistically at the nation's critical infrastructures and what can be done to enhance resiliency and reliability. It is important that we work with other parties in the private and public sectors to address these issues sufficiently."
Catherine Allen, CEO, BITS

Another issue underscored by the 9/11 attacks was the need for regional coordination. According to Allen, New York City had an experienced office of emergency management with extensive relationships and processes in place prior to the attacks; however, most other metropolitan areas did not. Forward thinking executives from financial institutions in Chicago recognized that city's vulnerabilities. They sought BITS' assistance in creating a regional coalition, and with support from the U.S. Department of Treasury, the coalition eventually became ChicagoFIRST (see article on Page 9). This model has led to the ongoing creation of regional coalitions around the nation.
(Continued, Page 3)

Catherine A. Allen serves as CEO of BITS, a nonprofit, CEO-driven financial services industry consortium made up of 100 of the largest financial institutions in the U.S. BITS works to leverage the intellectual capital of its members, fostering collaboration to address emerging issues where financial services, technology, and commerce intersect. BITS' priority issues include cybersecurity, crisis management coordination, fraud reduction, identity theft, IT outsourcing, and payments strategies.

BITS (*Cont. from Page 2)* In the area of interdependencies, BITS has focused on three sectors that are of great concern to the finance sector: telecommunications, electricity, and information technology. By regulation, banks are required to be up and running within a prescribed number of hours after a disruption. Without telecom, back-up power, or IT, that would be very difficult. So BITS got to work coordinating with these sectors to identify interdependencies and to find solutions for keeping channels open into financial institutions during an emergency.

Through work with the National Security Telecommunications Advisory Committee, the Network Reliability and Interoperability Council, the Alliance for Telecommunication Industry Solutions, telcos, the National Communications System, and telecom industry groups, the sector has identified, and in some cases mapped out, diversity and redundancy issues. From the information gathered by these mapping exercises, BITS has developed a best practices document for what financial institutions should be asking of their telecommunication providers. (The BITS Guide to Business-Critical *(Continued, Page 13)*

PREPARE

BITS created a list of seven key elements that the U.S. government should support to secure the nation's IT assets. These elements form the acronym, PREPARE.

Promote. Government can play an important role in promoting the importance of secure information technology. Also, government should do more to facilitate collaboration among critical infrastructure sectors and government.

Responsibility. Government should promote shared responsibility between suppliers and end users for developing, deploying, and maintaining secure information networks. Government can play an important role in establishing incentives and making producers of software and hardware accountable for the quality of their products.

Educate. Communicate to all users of information technology the importance of safe practices. Public confidence in e-commerce and e-government is threatened by malicious code vulnerabilities, online fraud, phishing, spam, spyware, etc. Ensuring that users (home users, businesses of all sizes, and government) are aware of the risks and take appropriate precautions is an important role for government and the private sector.

Procure. Using its purchasing power and leveraging security requirements and best practices developed by the public and private sectors, government can play an important role in encouraging the IT industry to deliver and implement more secure systems.

Analyze. Government should collect information and analyze the costs and impact of information security risks, vulnerabilities and threats and provide this analysis to policy makers.

Research. Government can play an important role in funding R&D in the development of more secure software development practices, testing and certification programs. In addition, training future generations of programmers, technicians and business leaders that understand and manage information security can be accomplished by establishing university and educational/certification programs.

Enforce. Law enforcement must do more to enforce, investigate and prosecute cyber crimes here and abroad.

Hurricane Katrina: Infrastructure Protection in Action

Excerpted from the Financial Services Sector Coordinating Council for CIP and Homeland Security's *Protecting the U.S. Critical Financial Infrastructure: 2005 in Review*

The financial community's response to the series of hurricanes that devastated the U.S. Gulf Coast during the year demonstrated the sector's enhanced resilience. It also highlighted the extensive degree to which public and private organizations communicated and cooperated to mitigate the effects of the disasters, clearly illustrating the dramatic improvement of the past few years in forging a public-private partnership to protect the country's financial infrastructure.

These record-breaking storms - particularly Hurricane Katrina - severely damaged communities in the region and led to widespread disruption of services and displacement of people. The challenges to the financial community were threefold: to determine the impact of the devastation on financial services organizations in the area, to create and execute a plan for restoring financial services to affected citizens while still maintaining appropriate levels of financial risk, and to aid in the resumption of financial services and supporting a return to normal business operations. The sector succeeded in meeting these challenges, with private and public sector organizations working jointly to coordinate their response.

The agencies of the Financial and Banking Information Infrastructure Committee (FBIIC), under the Treasury Department's leadership, coordinated assessment and restoration activities, as well as efforts to communicate to the financial community much-needed information about the status of the affected areas. Institutions in the storm-damaged regions, those that had local branches there, and others that were dependent on firms in the area, were kept informed about recovery efforts, progress being made, locations of new branches being set up outside the impacted area, resettlement sites, methods for verifying identities of people with no identity documents, and a multitude of other details to help restore services to everyone affected by the storms. In addition, this collaborative effort enabled regulatory agencies to quickly reach institutions with guidance allowing them to defer or modify specific regulatory requirements in light of the seriousness of the situation. The Federal Deposit Insurance Corporation (FDIC) and the National Credit Union Administration (NCUA) played a key role in broadly disseminating specific information about the status of individual financial institutions in the affected areas, permitting sector members to monitor the situation as it unfolded.

This information was communicated from Treasury and FBIIC agencies *(Continued, Page 14)*

In May 2005, U.S. Treasury Secretary John Snow announced the appointment of the Depository Trust and Clearing Corporation's Chief Operating Officer **Donald F. Donahue** as Sector Coordinator for Banking and Finance, to work with Treasury to help protect the nation's critical infrastructure in the financial services sector. This entails leadership of the Financial Services Sector Coordinating Council for Critical Infrastructure Protection (FSSCC), which Donahue has been a member of since it was created in 2002. The FSSCC, formed under a Homeland Security Presidential Directive, is a private-sector organization that fosters industry initiatives to strengthen the nation's infrastructure.

FSSCC Says Avian Flu Outbreak Poses Unique Threat

Council Issues Paper Outlining Guidelines to Prepare Financial Industry

A serious outbreak of illness such as avian flu could cause problems for business and the financial services industry that are quite distinct from the business continuity issues posed by disruptions associated with natural disasters, according to a paper issued in January by the Financial Services Sector Coordinating Council for Critical Infrastructure Protection and Homeland Security (FSSCC).
In the paper, which discusses issues that financial institutions may need to face in the event of a widespread avian flu outbreak, the FSSCC said that a number of financial institutions are concerned that their current planning for business continuity may not address the unusual circumstances that could arise during an outbreak of flu or other highly infectious disease.

For example, according to the council's paper, a serious avian flu outbreak could erupt in waves over weeks or even months, with some waves appearing to be mild only to be followed by others that are much more severe.

"Even after a particular wave appears to subside, follow-up waves could develop after safeguards are relaxed," the paper said, suggesting that the timeframe for coping with an epidemic could be much longer than the U.S. has experienced in dealing with natural disasters.

As a result, according to the paper-"Issues for Consideration Regarding Preparation for Avian Flu"- organizations may have to deal with significant absenteeism for weeks at a time from illness, family demands or fear of contagion. Personnel absences may become extensive enough to require firms to alter contingency plans for maintaining critical operations.

Compounding the problem, the paper notes, is that if an avian flu outbreak reaches epidemic proportions, it's likely to affect multiple regions of the country and the globe at the same time. Consequently, the paper says, "the backup facilities that many financial organizations have established - even remote sites hundreds of miles distant from primary facilities - may be just as affected by the outbreak as the primary locations they are intended to back up."

Another consideration that financial service organizations need to plan for, the paper said, is that the same absenteeism issues are likely to spread to power systems, transportation, telecommunications, waterworks - even police, fire and emergency medical services. These types of problems would present additional complications for contingency planning that firms need to address.

"It's important to point out," noted Donald F. Donahue, Chairman of the FSSCC and Sector Coordinator for Banking and Finance, "that, at this time, an epidemic or pandemic of avian flu 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 for us to take.
Even if a highly communicable form of avian flu develops," Donahue said, "we do not know how virulent the virus would be, nor how serious its effects would be."

The council cautioned that financial service organizations ought to reexamine their current business continuity plans with an eye to surviving a long-running outbreak of a highly infectious disease. The FSSCC recommendations for organizations are listed in the box on Page 6.

While some scenarios suppose that an outbreak would first occur overseas so that U.S. organizations would have some advance warning, it is quite likely that the actual warning period prior to an outbreak in the United States could be brief, the council said in its statement.

FSSCC is issuing this paper, Donahue explained, to share some of the thinking evolving in the financial service industry about how *(Continued, Page 6)*

Avian Flu *(Cont. from Page 5)*
issues raised by an epidemic or pandemic "are quite distinct" from issues posed by natural disasters or deliberate malicious activity.

"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," Donahue said.

A copy of the FSSCC statement and paper on Avian Flu can be accessed at http://www.fsscc.org/reports/avianflu.html. ❖

Sector Recommendations for Possible Avian Flu Outbreak

- Identifying which operations could be suspended and which are critical, keeping in mind that activities such as payroll and administrative functions, which are often suspended during short-term disasters or emergencies, may need to be kept functioning in order to sustain the organization.
- Splitting and segregating critical staff into separate offices or locations, and planning for possible governmental actions (such as school closings or travel restrictions) that would cause larger numbers of staff to stay home.
- Expanded telecommuting, although that raises issues such as costs, advance preparations and even the sustained quality of online services during a long-term outbreak.
- More use of teleconferencing and videoconferencing to avoid travel and the need for face-to-face meetings.
- Limits on long-distance travel and the possible need for special local travel arrangements for critical staff commuting to and from workplaces.
- Stepped up security because police and other security services may be compromised by illness and absenteeism.
- More timely information-gathering systems to keep track of employee absenteeism or work-at-home situations.
- Emergency plans that can be phased in to deal with various degrees of an influenza outbreak, both locally and on a broader basis.
- Communication strategies to prepare statements in advance and to reach employees and inform external parties such as regulators, customers, suppliers, trading parties and the public.
- Coordination with local emergency management organizations in order to track such potential governmental actions as shutdowns of public transportation, or the imposition of "snow days" to limit public exposure to the virus.
- Employee health and safety issues, including reliable information sources for the latest medical developments, medical or other health care expertise, and vaccination programs.
- Testing and monitoring programs to scan for possible employee contagion or infection, or to isolate employees who become suddenly ill.
- Legal review of business continuity and employee safety arrangements to ensure compliance with personnel and privacy laws and regulations.
- Budget and administrative questions, such as the stockpiling of supplies or advancing administrative leave to large numbers of employees.

Financial Services Information Sharing and Analysis Center

As the Financial Service Information Sharing and Analysis Center (FS/ISAC) continues to grow and provide a greater depth of services to its constituent members, it remains focused on its core mission of gathering threat, vulnerability, and risk information about cyber and physical security risks. This critical information, once analyzed by industry experts, is then distributed as an alert containing a description of the threat or vulnerability, its severity, and recommendations for solutions. Originally launched in 1999 to aid the sector in preparation for Y2K, the ISAC has since expanded its membership by using multiple tiers of membership and working closely with industry associations. Through the membership and license agreements with trade associations, the FS/ISAC is delivering urgent and crisis alerts to eligible firms that make up the majority of banking assets and securities transactions in the United States.

The FS/ISAC is managed by a Board of Directors, with each board member serving a three-year term, elected by the Premier and above Members. The board elects officers for two year terms. (See listing of all Board Members included below). In 2005 three board members stepped down, Larry Bickner of Bank of America, Tom Foster of Fannie Mae and Melissa Rockhill of Merrill Lynch. These three served multiple terms and made major contributions to the FS/ISAC. The membership elections held in October saw Dave Cullinane of Washington Mutual, Ronald Green of Bank of America, and Gary Owen of Citigroup join the board. Additionally, following Byron Yancy's retirement, Bill Nelson *(Continued, Page 12)*

Board of Managers

Chairperson: *Suzanne Gorman*, Managing Director, Corporate Information Security, Securities Industry Automation Corporation

Vice Chairperson: *George S. Hender*, Vice Chairman, The Options Clearing Corporation

Treasurer: *Eric Guerrino*, Senior Vice President, The Bank of New York

Board Members

Byron Collie, Vice President, Global CERT Coordinator, Goldman Sachs

Dave Cullinane, CISO, Washington Mutual

Ronald Green, SVP, Investigations and Digital Discovery, Bank of America

Gary Owen, VP ISS/SIRT Director, Citigroup

Gary Reynolds, SVP/Dir Financial and Electronic Crime Inv, Wells Fargo

Louis Rosenthal, Executive Vice President, ABN AMRO Services Company

Ty R. Sagalow, Esq., Executive Vice President, eBusiness Risk Solutions, American International Group, Inc.

Robert Vitali, Executive Director, Chief Information Security Officer, Morgan Stanley

Administration

Bill Nelson, Executive Director FS/ISAC

Frank Treu, FS/ISAC Program Manager, Sr. Manager, ISAC Intelligence Services, VeriSign

John Basta, FS/ISAC Coordinator, VeriSign

Fran Coppola, FS/ISAC Administrator, DTCC

Fifteen Financial Institutions, Vendors, and Organizations Convene to Tackle Business Continuity Issues

The Financial Services Technology Consortium (FSTC) recently announced that 15 leading financial institutions and technology companies have undertaken its Resiliency Model Project, whose goals are to create, for the first time, benchmarks for operational resiliency traversing all areas of a financial enterprise.

"Financial institutions clearly recognize the importance of having plans and methodologies in place to ensure business continuity in the event of an unforeseen circumstance or disaster," said Dan Schutzer, Executive Director of FSTC. "Currently, there are no industry-wide benchmarks against which institutions can measure their resiliency performance and make investment decisions. The results of this effort will be invaluable to the industry going forward."

This project addresses the critical need for institutions to adequately plan and measure their resiliency activities against a set of industry standards and establish a process improvement roadmap. This project is a follow-on to the highly successful Business Continuity Compliance that concluded in June 2005 and the Resiliency Model Project Phase I which concluded in November 2005. The Business Continuity Compliance project clarified a confusing web of 100 global continuity regulations, standards and guidelines affecting U.S. financial institutions. The team analyzed content, identified commonalities and differences, and examined trends. Phase I of the RM project identified and documented the essential capabilities of operational resiliency, developed a road map toward an eventual process improvement framework, and began the process of creating a common resiliency taxonomy, outlined a process improvement framework for resiliency capabilities, characteristics and goals of sustainability management, and defined resiliency terminology.

The second phase of the RM project will continue the team's groundbreaking work. The participating institutions will work together to document the goals and practices of vital operational resiliency processes and develop a draft process improvement framework. The second phase of the Resiliency Model initiative will also develop requirements for resiliency metrics and measurements and explore ways in which the process improvement framework can be used to assess an organization's operational resiliency capability. The overall goal of the Resiliency Model project is to define a process improvement approach for operational resiliency that a full spectrum of industries and organizations can utilize to improve their security, business continuity, and resiliency efforts.

"The level of interest in this important project has been outstanding," said Charles M. Wallen, Managing Executive of FSTC's Business Continuity Standing Committee, and project director. "Financial institutions and their technology solution providers have joined forces to work together to develop a methodology that will allow organizations to measure and monitor their resilience against a common standard."

FSTC has partnered with the Carnegie Mellon Software Engineering Institute. The SEI's CERT Program is conducting applied *(Continued, Page 15)*

Under the chairmanship of **Donald T. Parker**, the Financial Services Technology Consortium (FSTC) sponsors noncompetitive collaborative research and development of interbank technical projects affecting the entire financial services industry. The FSTC's mission is to help its members collaborate on technical and business aspects of technologies so that they may rapidly bring innovations in service and quality closer to the marketplace and to their customers, while competing upon a bedrock of sound, shared technology fundamentals.

ChicagoFIRST

"Because a Crisis is No Time to Exchange Business Cards"

Recognizing that natural disasters and terrorist attacks have their greatest impact in the region in which they occur, financial institutions in the Chicago area formed a coalition for business continuity in 2003. The coalition, ChicagoFIRST, is dedicated to enhancing the resiliency of the financial community in the Chicago metropolitan region. ChicagoFIRST accomplishes this by fostering business recovery coordination and planning among its members and implementing a public/private partnership between its members and government at all levels.

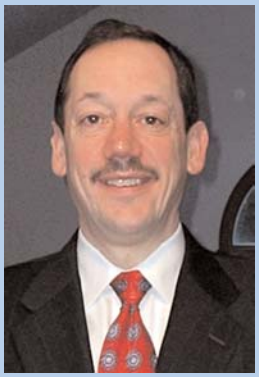
The members of ChicagoFIRST include futures and options exchanges, commercial banks, brokerage firms, and clearing organizations. In January 2004, the organization became a limited liability company owned by the following firms: LaSalle Bank/ABN AMRO; Chicago Board Options Exchange; Chicago Mercantile Exchange; The Northern Trust Bank; UBS Warburg; Harris Bank; Archipelago; Chicago Stock Exchange; BankOne; William Blair & Company; Mesirow Financial; Mizuho Securities; The Options Clearing Corporation; and Bank of America.

ChicagoFIRST Activities

Crisis Communication. ChicagoFIRST's highest priority had been to obtain a seat at Chicago's Joint Operations Center (JOC) to facilitate crisis communication. With the help of the Treasury Department, ChicagoFIRST achieved this goal in 2003. This gives the coalition's representative first-hand information about any disaster or emergency and how the city plans to respond. ChicagoFIRST has policies and procedures for use of the seat and has identified individuals from the ChicagoFIRST membership to staff the center on a 24x7 basis when the Department of Homeland Security elevates its alert level to orange or red, or the JOC is otherwise activated by local authorities. Additionally, crisis management and coordinating procedures with the center are periodically being tested.

Credentialing. In the aftermath of the September 11 attacks, essential personnel whose physical premises were not destroyed lacked pre-authorized (by local officials) physical credentials to access restricted areas. Many businesses were unable to re-open in a timely

(Continued, Page 15)



Brian Tishuk became the first Executive Director of ChicagoFIRST in 2004. He is responsible for forging a relationship between the financial institution members and government at all levels and for developing best practices for business continuity.

Prior to that, he enjoyed a career at the United States Treasury Department during which he addressed a vast array of public policy issues affecting financial institutions, from the savings and loan crisis of the mid-1980s to the attacks of September 11th, 2001.

Following September 11th, Mr. Tishuk led The Treasury's efforts to enhance the resiliency of financial institutions, establishing the Office of Critical Infrastructure Protection and Compliance Policy and serving as its Acting Director and Deputy Director. Focusing attention on financial institutions in other parts of the country, Brian initiated a Treasury outreach effort that both encouraged and facilitated cooperation among financial firms in Chicago, which led to the formation of ChicagoFIRST.

ChicagoFIRST just hired a deputy director, Sara Alexander. Prior to her new position with ChicagoFIRST, Alexander was the Assistant Director of Emergency Management for the City of Chicago Office of Emergency Management and Communications (OEMC).

Legal Insights

Update: Legal Actions Based on Information Security Breaches

by Maeve Dion

CardSystems Solutions, Inc.

CardSystems processes authorizations of credit and debit card purchases for numerous small and mid-size merchants. In contravention of credit card company security standards, the CardSystems database retained unencrypted data from the magnetic stripes ("track data") of cards for certain transactions that had not been completed. CardSystems' CEO testified at a Congressional hearing that the track data was retained so that CardSystems could later analyze the data to determine why the transactions were not successful. In September of 2004, an unauthorized third party accessed CardSystems via an internet-based application used by CardSystems' customers, and placed a script on the CardSystems platform. Specifically targeting the track data, the script extracted the data and exported it to an FTP site. Forensic audits showed that data was only exported once, on May 22, 2005. Although initial reports indicated 40 million accounts may have been compromised, counsel from MasterCard and CardSystems testified at a Congressional hearing that a subsequent forensic audit showed that data from 239,000 accounts had been exported. Other credit card company representatives testified at the same hearing that the personal information held in CardSystems' database *did not include* dates of birth, addresses, telephone numbers, social security numbers, or driver's license numbers. Congressional testimony also revealed that, although CardSystems' retention of personal information (since 1998) and its failure to encrypt the data violated credit card company security standards and contractual agreements, a third-party security audit of CardSystems in 2004 (performed in order to qualify CardSystems to process Visa purchases), failed to identify these vulnerabilities.

Federal Trade Commission's Proposed Settlement. (*In re CardSystems Solutions, Inc.*, FTC, File No. 0523148):

- This was the first FTC "unfair practice" enforcement action against a credit card processor. FTC alleged "that CardSystems:
  - created unnecessary risks to the information by storing it;
  - did not adequately assess the vulnerability of its computer network to commonly known or reasonably foreseeable attacks, including "Structured Query Language" injection attacks;
  - did not implement simple, low-cost, and readily available defenses to such attacks;
  - did not use strong passwords to prevent a hacker from gaining control over computers on its computer network and access to personal information stored on the network;
  - did not use readily available security measures to limit access between computers on its network and between its computers and the Internet; and
  - failed to employ sufficient measures to detect unauthorized access to personal information or to conduct security investigations."

- CardSystems agreed to (1) establish and maintain an information security program with reasonable administrative, technical, and physical safeguards; (2) obtain a third-party security audit within 6 months of the consent order and every-other year for the next 20 years, and provide the audit results and relied-upon documentation to the FTC within 10 days of each audit report; and (3) maintain (and make available to the FTC) records of the biennial audits and any other documents that "contradict, qualify, or call into question" CardSystems' compliance.

Read more at http://www.ftc.gov/os/caselist/0523148/0523148.htm.
(Continued, Page 11)

Legal Insights *(Cont. from Page 10)*

Class action lawsuit brought by cardholders and card-accepting merchants. (*Parke v. CardSystems Solutions, Inc.*, No. CGC-05-442624, Superior Court of California, County of San Francisco):

- Causes of action include negligence, unfair and deceptive business practices, and violations of California's data breach notification law.
- Complaint available on website of plaintiffs' counsel: http://www.techfirm.com/cardsystems.pdf.
- Case actions (including defendants' answers) available via http://www.sftc.org/.

Other Legal Actions

Standard of Care under Gramm-Leach-Bliley. A student loan services company had a comprehensive security program that identified foreseeable security risks and implemented safeguards to control the risks. Thus, when (1) unencrypted personal customer information was kept on an employee's laptop, (2) the laptop was taken home with the employee, and (3) the laptop was stolen during a residential burglary, the company had not breached GLBA standards. *Guin v. Brazos Higher Educ. Serv. Corp.*, Civ. No. 05-668 (RHK/JSM), 2006 U.S. Dist. LEXIS 4846 (D. Minn., Feb. 7, 2006). Also available at http://www.nysd.uscourts.gov/courtweb/pdf/D08MNXC/06-00529.PDF.

Costs of Third Party Injuries Support Computer Fraud and Abuse Act Prosecutions. Another circuit has recognized the validity of CFAA prosecutions that use third party damages to meet the statutory $5,000 minimum requirement (i.e., the third party was injured by unauthorized access to a computer system owned by someone else). The Eighth Circuit found that IBM's costs of fixing its client's computer system after the intrusion could be included as damages supporting the conviction. *United States v. Millot*, 433 F.3d 1057 (8th Cir. 2006). Three years earlier, the Ninth Circuit found that the plaintiff had a CFAA claim against the defendant who, in the course of the underlying commercial litigation, had obtained the plaintiff's emails via an unlawfully issued subpoena to which the plaintiff's Internet service provider responded. *Theofel v. Farey-Jones*, 359 F.3d 1066 (9th Cir. 2003).

Acxiom Hacker Sentenced to Eight Years. Last August, Scott Levine was found guilty of various charges resulting from his 2003 hacking and theft of **1.6 billion** customer records in Acxiom databases. At the time, Acxiom's clients included 14 of the 15 biggest credit card companies and five of the top six retail banks. FBI Press Release regarding Levine's sentencing: http://littlerock.fbi.gov/dojpressrel/pressrel06/datatheft022206.htm. ❖

Protecting the Financial Sector: A Public and Private Partnership

The Federal Deposit Insurance Corporation is in the midst of hosting a series of symposia around the nation to discuss critical infrastructure protection, regional coalitions, physical and cyber threats, risk management, and emergency preparedness. The meetings are co-sponsored by the government's Financial and Banking Information Infrastructure Committee and the private sector's Financial Services Sector Coordinating Council.

Meetings have been held in such places as New Orleans, St. Louis, Anchorage, and Oklahoma City. Upcoming meetings are planned for Philadelphia and San Juan, Puerto Rico. Please visit the FDIC's website at http://www.fdic.gov/news/conferences/index.html for more information.

The Federal Deposit Insurance Corporation (FDIC) preserves and promotes public confidence in the U.S. financial system by insuring deposits in banks and thrift institutions for up to $100,000; by identifying, monitoring and addressing risks to the deposit insurance funds; and by limiting the effect on the economy and the financial system when a bank or thrift institution fails.

An independent agency of the federal government, the FDIC was created in 1933 in response to the thousands of bank failures that occurred in the 1920s and early 1930s. Since the start of FDIC insurance on January 1, 1934, no depositor has lost a single cent of insured funds as a result of a failure. ❖

NCRFirst

Like the banking and finance communities in Chicago and Miami, the National Capital Region's (NCR) sector has critical shared concerns, including business continuity, obtaining timely and accurate information, employee safety, and preparedness planning. The sector recognizes that there is currently no mechanism or single organization to directly address these issues across the region. The CIP Program's National Capital Region - Critical Infrastructure Project (NCR-CIP) organized sector focus group meetings to address these issues and unanimously agreed to adopt the ChicagoFIRST model for the National Capital Region. Subsequently, the Department of Treasury recently hosted an "NCRFirst" formation meeting, with briefings from Brian Tishuk of ChicagoFIRST, Scott Parsons of Treasury, Wayne Abernathy of the American Bankers Association (ABA), and Doug Johnson (also of the ABA).

The next meeting is planned for April, when a chair and co-chair will be selected and task forces formed. A briefing by a MiamiFirst representative is also planned. Please contact Andrew Rushing, Senior Policy Analyst, Office of Critical Infrastructure Protection and Compliance Policy, Department of Treasury at (202) 622-9335 or via email Andrew.Rushing@do.treas.gov, for more information.

For additional information on the NCR-CIP Banking and Finance Sector report please visit the website at http://cipp.gmu.edu/news/story.php?id=113 or contact Christine Pommerening at (703) 993-3132; cpommere@gmu.edu.

FS/ISAC *(Cont. from Page 7)* was selected by the Board to be the new Executive Director of the FS/ISAC. Nelson spent the last eighteen years building NACHA, the Electronic Payments Association, a rulemaking body for the ACH Network. During his tenure at NACHA, Bill was responsible for growing the use of electronic payments for direct deposit, direct debits, business-to-business, electronic check conversion and WEB and telephone-initiated payments. He also was responsible for implementing a number of risk management and compliance initiatives to improve the quality of the ACH Network, which processed close to 14 billion payments in 2005. Prior to joining NACHA, Bill worked for Mellon Bank in its Global Cash Management Division.

Membership in the FS/ISAC reached a record high in 2005, climbing to nearly 1,800 participants (a 200% increase from 2004) and reaching 34% of the industry. In 2005, the group launched CINS, or Critical Infrastructure Notification System, providing a best-in-class, highly reliable, highly available notification service with rapid completion of phone calls to end users. The system delivers voice messages, text-to-voice converted messages, and text to end users, requiring users to confirm delivery. This allows the ISAC to report, in real-time, the percentage of the financial services sector informed of a critical issue or event. The system was used twice in 2005: for a critical software patch advisory in April and minutes after the London bombings on July 7. ❖

Suzanne Gorman is Chairperson of the FS/ISAC

BITS *(Cont. from Page 3)* Telecommunications Services can be viewed at http://www.bitsinfo. org).

Similarly, BITS has worked with the Critical Power Coalition and Power Management Concepts to develop a guide that provides financial institutions with industry best practices for understanding, evaluating and managing risks associated when the predicted reliability and availability of the electrical system is disrupted. Further, it outlines ways financial institutions can enhance reliability and ensure uninterrupted back-up power. The BITS Guide to Business-Critical Power will be published at the end of April.

For information technology, BITS has targeted the five most important software and hardware companies critical to resiliency in the finance sector and is creating strategic partnerships with them. The goal of these partnerships is to identify how the IT sector can address the finance industry's business continuity and resiliency requirements.

Allen says that the sector's extensive work in other areas such as identity theft and fraud are not only useful for consumers, but for combating terrorism as well. All of these efforts go back to the issue of resilience, and making sure that institutions are aware of the threats and have best practices in place.

The finance sector's most recent test of its preparedness came during Hurricanes Katrina and Rita last fall. The sector found that it fared well due to the mechanisms that it had in place for communications and coordination. The Financial Services Sector Coordinating Council facilitated communications between industry and regulators during the crisis so there was a good amount of information sharing. People were able to access cash and none of the banks were down with regard to processing and settlement of payments and funds. Those that were physically unable to keep their doors open remained open online.

Two of the major issues that the sector had to deal with were contamination and fraud. The sector had to figure out how to deal with contaminated cash and lock boxes, and is now working on policies for addressing these unprecedented issues. As for fraud, BITS has a steering committee focused on the issue. At a minimum, the aftermath of the hurricanes allowed the sector to hone its skills in dealing with fraud.

One of the hot topics that can currently be heard on BITS' monthly crisis management conference calls is the pandemic avian flu, and the interdependency issues that arise from the possibility of large portions of the sector's work force telecommuting. BITS believes that the government could play an important role here, as in other issues that this sector, and other critical infrastructure sectors are trying to address.

Almost five years since the 9/11 attacks, BITS has not rested in its ongoing pursuit to address the multitude of layers in resiliency, business continuity, and critical infrastructure coordination. Due largely to BITS' work, the finance sector remains at the forefront of critical infrastructure protection and coordination. ❖

BITS recently launched the **Financial Institution Shared Assessments Program**. This program provides efficiencies and cost savings to financial institutions in evaluating IT service providers. Through a comprehensive questionnaire and objective and consistent assessment process, the Financial Institution Shared Assessments Program gathers detailed information on a service provider's controls (people, process, and procedures) and tests those controls. Six major national banks and several major providers have signed on to the voluntary program, which will greatly reduce costs for both sides. The program creates a framework for developing best practice guidelines, and is aimed at helping financial institutions in a regulatory environment. If a service provider suddenly fails, a bank is still accountable for its operational ability. By assessing a provider's controls, a financial institution can mitigate the risk to its IT infrastructure.

On the vendor side, the shared assessments program helps to keep costs down by allowing a provider to complete one assessment acceptable to numerous institutions, versus a separate assessment for each potential client.

The Financial Institution Shared Assessments Program is managed by The Santa Fe Group, a strategic consulting company providing expertise to leading financial institutions and other critical infrastructure companies. Founded in 1996 by BITS CEO Catherine Allen, The Santa Fe Group is a strategic partner to BITS. The Santa Fe Group serves clients on issues related to cybersecurity, critical infrastructure protection, fraud reduction, and payments strategies. Through a network of handpicked thought leaders and innovators, The Santa Fe Group's clients have access to the most advanced thinking in the industry.

Hurricane Katrina *(Cont. from Page 4)* through FSSCC and FS/ISAC to the financial industry at large, with private sector questions and concerns flowing back through the same channels for consideration and response. In addition, individual FSSCC member associations provided extensive communications to and support for their members, relaying information to public-sector authorities for action, where needed. Several days after Katrina's impact, FSSCC issued a public press release to reassure policy makers, the public and the media of the status and response of the financial sector. The FS/ISAC played a lead role in disseminating information about cross-sector issues and actions, ensuring that sector members were informed as efforts to recover telecommunications and power proceeded. The aftermath of Katrina and the other hurricanes demonstrated yet again the sector's effectiveness in marshalling its efforts and resources in times of emergency to restore the ability of U.S. citizens to conduct their financial affairs.

Cross-Sector Coordination and Response

The process of recovering from Hurricane Katrina also provided a graphic illustration of the interdependencies among critical infrastructure sectors. During the early days of the recovery, a key issue was getting cash to the affected areas through armored carriers and other delivery vehicles. Adequate fuel supplies were critical to this effort (a dependency on the energy sector), as were clear roads (a dependency on both the transportation and electric power sectors, as downed power lines had to be removed). Electric power and telecommunications capabilities were needed for operating ATMs to distribute the money. These sectors, in turn, had their own dependencies - for example, the electric power sector needed oil and gas supplies to run equipment. The recovery process dramatically underscored the myriad interconnections among critical sectors, highlighting the need to identify and clarify interdependencies and develop contingency plans to mitigate the failure of one or more of those links.

FSSCC documented a series of lessons learned from the Katrina recovery and communicated these to the Treasury Department and FBIIC in November 2005. From these lessons, FSSCC developed a number of recommendations, including the following:

- Many of the special processes and regulatory actions implemented after Katrina should serve as a template for other emergency situations. FSSCC urged the Federal agencies to compile an inventory of such activities.
- Actions by the FDIC and NCUA in communicating information on institutions' status should also serve as a model in future emergencies.
- Details of the special programs used to distribute emergency relief funds or financial assistance should be institutionalized for future use, as well.
- Local "credentialing" programs, permitting private sector infrastructure personnel access to affected areas for recovery activities, should be promoted and a general standard for such credentials implemented so that personnel from different areas of the country can quickly be deployed to help recovery efforts. ❖

FSTC *(Cont. from Page 8)* research in the application of process improvement techniques to information security and operational resiliency.

"CERT's objective is to help organizations to approach operational resiliency in a systematic, predictive manner through the collaboration of disciplines in security, business continuity, disaster recovery, and IT operations management, " said Rich Caralli, senior member of the technical staff at CERT.

FSTC brings together diverse and often competitive financial institutions, industry services providers, government agencies and others to collaborate and find solutions to key industry challenges. Project topics come from member financial institutions and are driven by participating members with the support of the FSTC staff. ❖

ChicagoFIRST *(Cont. from Page 9)* manner or had great difficulty doing so. As a result, ChicagoFIRST has established a working project team with the City of Chicago, the City of Chicago Police Department, and Chicago's Building Owners and Management Association to develop an interim system to credential essential individuals. The City of Chicago has adopted a credentialing pilot in which ChicagoFIRST participates.

Evacuations/Sheltering in Place. ChicagoFIRST is working closely with the City of Chicago and the State of Illinois to both understand how the region will evacuate the central business district, if necessary, and ensure that the financial community's procedures complement those of the government. The organization has also participated in exercises with the City to test evacuation procedures, and more exercises are planned.

Working Groups. ChicagoFIRST has launched five working groups, including the Security Working Group, Power Working Group, Telecommunications Working Group, Public Relations Working Group, and the Crisis Communications Working Group.

ChicagoFIRST is the Regional Model. BITS, the Treasury Department, and the Financial Services Sector Coordinating Council (FSSCC) consider ChicagoFIRST a model that can be productively employed in other regions of the country. The structure and degree of formality can be tailored to meet the needs of any regional financial community. ChicagoFIRST has committed to work with BITS, the Treasury Department, and FSSCC to assist any such efforts and to foster the development of other regional organizations. ❖

The CIP Program is directed by John A. McCarthy, a member of the faculty at George Mason University School of Law. The CIP Program works in conjunction with James Madison University and seeks to fully integrate the disciplines of law, policy, and technology for enhancing the security of cyber-networks, physical systems and economic processes supporting the nation's critical infrastructure. The CIP Program is funded by a grant from The National Institute of Standards and Technology (NIST).

The CIP Report is published by Zeichner Risk Analytics, LLC on behalf of the CIP Program. ZRA is the leading provider of risk and security governance knowledge for senior business and government professionals. ZRA's vision is to be a consistent and reliable source of strategic and operational intelligence to support core business processes, functions, and assurance goals.

If you would like to be added to the distribution list for *The CIP Report*, please click on this link: http://techcenter.gmu.edu/programs/cipp/cip_report.html.