Contingency Planning in ICSA Member Countries

Australia

In an effort to review and upgrade Australia's capacity to deal with threats to critical infrastructure, the government has formed a Trusted Information Sharing Network for Critical Infrastructure Protection (TISN), under which contingency plans are being developed for strategically important sectors, including banking and finance. The Federal Attorney General's Department is coordinating this work with input from the Critical Infrastructure Advisory Council (CIAC) and the National Counter-Terrorism Committee (NCTC). For further information see: www.cript.gov.au

In the finance sector, responsibility for banking system stability rests with the Reserve Bank of Australia (RBA), which is specifically responsible for the payments system, and the Australian Prudential Regulation Authority (APRA), which is responsible for the prudential supervision of individual financial institutions. These authorities, along with the Australian Securities and Investments Commission (ASIC), are working with each other and with banks and other financial institutions to ensure that adequate business continuity programs are in place. APRA also works closely with the Allfinance Business Continuity and Disaster Recovery Forum, an industry group established in 2002 to develop and share best practices for disaster recovery and business continuity planning. These agencies also participate in the Australian Government's Critical Infrastructure Protection arrangements.

Canada

The Investment Dealers Association of Canada (IDA) is working on contingency planning for the financial services sector, specifically through the establishment of a "Crisis Center" for its members. IDA is also well advanced in establishing Minimum Disaster Recovery Planning Standards for members.

France

In France, each market infrastructure, ie Eurnonext, Clearnet, Euroclear, CRI has its own contingency planning. These entities have established committees with the large banks in order to cooperate and solve the problems when necessary. Regulators require each market infrastructure to test its contingency plan with its members twice a year. At the national

level, the Commission Bancaire has done work regarding contingency planning for information systems in the banks.

Japan

Japanese securities firms are not required to prepare their own business continuity plans. However, there is a category in the "Inspection Manuals for Securities Firms" by the Financial Services Agency (FSA) which allows the FSA to check whether securities companies have contingency plans in place. The manuals are the guidebook used by the FSA's inspectors in examining securities companies. The Manuals stipulate that firms have in place anti-earthquake measures, remote storage facilities for data and contingency plans for other emergencies. In addi-tion, all plans and revisions must be approved by the firms' board of directors and firms must have a system in place for testing their emergency procedures. Firms in the financial securities sector are expected to ensure the soundness and appropriateness of their business by preparing their own Manuals according to their size and the nature of the work in which they are engaged.

Korea

At the national level, under the country's Securities and Exchange Act the Ministry of Finance and Economy is empowered to temporarily close securities markets or take other necessary measures in response to a natural disaster, warfare, a sudden and significant change in economic conditions or other incidents that would interrupt the normal flow of business. In addition, the individual exchanges are empowered to suspend trading during crisis situations.

In response to both domestic and external disturbances in 2001, the Financial Supervisory Service (FSS), Korea's financial securities supervisor, recommended that Korean securities firms create contingency plans for their internet operations and establish disaster restoration centers. The target recovery time for securities firms and securities authorities to have their systems operational after a natural disaster, technical problem or man-made catastrophe is three hours. It is expected that all Korean securities firm will have complied with this recommendation by the end of 2003.

Sweden

The Financial Supervisory Authority is in charge of contingency planning in the financial sector in Sweden. The authority has identified a number of strategic banks, securities companies and in addition the stock exchange and the CSD as strategic actors in the securities market. As part of its ordinary supervision measures, FSA is urging these institutions to undertake contingency planning. FSA has also organized certain catastrophic scenario training sessions with the institutions concerned.

In late 2002, the Swedish Securities Dealers Association (SSDA) organized a seminar for its members on the topic of contingency planning with assistance from international specialists in this field. Documentation from this seminar can be found on SSDA website: www.swedsec.com

United Kingdom

The UK's financial sector authorities – HM Treasury, the Bank of England and the Financial Services Authority (FSA) – maintain a tripartite Standing Committee on Financial Stability, comprising senior representatives of the three authorities. Following the events of September 11, 2001, the Standing Committee established a sub-group to focus on resilience and contingency planning that would coordinate the work being done by the public and private sectors on disaster recovery and business recovery planning. The three authorities also maintain a website on U.K. financial sector continuity planning that gives an overview of the main organizations involved in this work, their responsibilities and activities and a brief summary of the key issues being addressed. This website can be found at: www.financialsectorcontinuity.gov.uk/home/default.asp. A short paper that summarizes the work being done by financial authorities to promote the resilience of the U.K. financial sector was released in June 2003 and can be found on the website referenced above.

In early 2003, the U.K. Treasury issued a consultation paper, "The Financial System and Major Operational Disruption", in an effort to determine if new statutory powers should be sought to assist in promoting order in the financial system in extreme circumstances of operational disruption. The Government also requested comments about additional ways in which the financial authorities could usefully assist the private sector's work in making financial markets more resilient. The document can be found at: HM Treasury, The Financial System and Major Operational Disruption. The government has subsequently established a taskforce to examine the possible need for legislative powers in the event of major operational disruption to the UK financial system.

The FSA issued a consultation paper ("CP 142: Operational risk systems and controls") in July 2002 dealing with the management of operational risk that set out guidance on some of the main areas that a firm should

consider when managing operational risk, including business continuity management. CP 142 and a related policy statement issued by the FSA in March 2003 can be found on the FSA website, www.fsa.gov.uk (click on publications).

On the private sector side, the British Bankers' Association and KPMG launched a new Guide to Business Continuity Management for Financial Services in early 2003. The guide offers a step-by-step approach that businesses in the financial services industry can take including measures for assessment, design, implemen-tation, measurement and testing of their continuity planning and disaster recovery systems. It also includes case studies and advice from key industry players as well as regulators dealing with aspects of business continuity planning.

United States

Both the public and private sector have become actively involved in contingency planning for the U.S. financial system since the terrorist attacks of September 11, 2001. The three main governmental agencies concerned with the financial services sector -- the Board of Governors of the Federal Reserve System, the Comptroller of the Currency, and the Securities and Exchange Commission -- issued a revised joint white paper on business continuity planning in April 2003. The document, "White Paper on Sound Practices to Strengthen the Resilience of the U.S. Financial System," can be found at: Interagency Paper on Sound Practices to Strengthen the Resilience of the U.S. Financial System. Separately, the Government Accounting Office (GAO) issued a report on business continuity planning and the financial services industry in early 2003, which suggested additional ways to prepare for future potential business disruptions. The report is at: GAO, Potential Terrorist Attacks.

The U.S. Department of Homeland Security Homeland Security unveiled two new programs intended to safeguard the U.S. financial system in mid-2003. The first program, “Operation Cornerstone,” will increase the level of information sharing between the agency and the financial community (including semi-annual meetings with key financial services executives). The second initiative expands the Department’s electronic crimes task force, which investigates e-commerce and telecommunications fraud, identity crime, and other computer-intrusion crimes.

On the private sector side, the Financial Services Sector Coordinating Council (FSSCC) was formed in June 2002, to coordinate critical infrastructure and homeland security initiatives for the financial services

industry. The FSSCC website can be found at: www.fsscc.org. One of the FSSCC's roles is to represent the financial markets in coordination with the Financial and Banking Information Infrastructure Committee (FBIIC). The FBIIC, which is chaired by the U.S. Treasury's Assistant Secretary for Financial Institution, is a standing committee of the President's Critical Infrastructure Protection Board, serves as the Office of Homeland Security Financial Markets Work Group and is charged with coordinating federal and state financial regulatory efforts to improve the reliability and security of the U.S. financial system. The FBIIC's website can be found at: www.fbiic.gov

In addition, the privately funded Financial Services/Information Sharing and Analysis Center (FS/ISAC), which has the objective of increasing the security of the internet by sharing information on cyber attacks, vulnerabilities, and best practices, has developed an early warning system to notify banks and broker dealers of relevant information on potential threats to the financial system. The U.S. Treasury's Banking and Finance Sector Coordinating Committee on Critical Infrastructure Protection created the FS/ISAC in late 1999. Their website can be found at: www.fsisac.com/aboutus.cfm

The Securities Industry Association (SIA), a leading trade association for the securities industry in the United States, has issued best practices for business continuity plans. This document can be found at: Business Continuity Best Practices. In addition, SIA is currently carrying out a benchmark survey intended to determine the level of preparedness among member firms. The results of the survey will be released in September 2003.