

September 14, 2006

Criteria | Financial Institutions | General:
**ERM And Terrorism Risk For
Financial Services Firms**

Primary Credit Analysts:

Mark Puccia, New York (1) 212-438-7233; mark_puccia@standardandpoors.com
David Ingram, New York (1) 212-438-7104; david_ingram@standardandpoors.com

Table Of Contents

Operational Risk Management

Conclusion

ERM And Terrorism Risk For Financial Services Firms

Terrorist attacks, generally long in the planning and swift yet lethal in the execution, seek to cause as much primary and collateral damage (not to mention havoc) as possible. For the financial services industry, mitigating the risk also requires long-range plans to enable swift (but hopefully not lethal) execution and minimal havoc. The terrorist attacks that to date have targeted the financial services industry, such as the early 1990s bombings in London and New York and the World Trade Center's destruction in 2001, exposed the industry's substantial short- to medium-term vulnerability.

When assessing enterprise risk management (ERM) as a part of rating a financial services company, Standard & Poor's Ratings Services looks for preparedness across the enterprise. We would, of course, take into account a broad range of contingencies for each firm. Given how globalized the financial services industry now is, terrorism risk for this sector must be managed not only across an enterprise but also across the entire industry throughout the world. A terrorist attack can wreak serious damage at several levels to this globally interlocked industry.

In a geographically focused attack, financial services companies would experience the same physical plant and employee losses as companies in other industries would, and they could also endure very high levels of data loss or corruption. Resuming day-to-day commerce as soon as possible would require secure offsite data backup and storage as well as procedures to evacuate employees and essential materials to safety and then to the backup location.

We would also want to see the stress tests a company uses to estimate the potential impact of plausible terrorism scenarios, how (and how frequently) they use them to assess their exposure to terrorism risk, and how they track and manage that exposure.

This is not to imply that terrorism risk needs to be treated differently from similar catastrophic risks. Other extreme events—including hurricanes/typhoons, earthquakes, pandemics, severe winter storms, and tsunamis—can result in significant business disruption and should be provided for in business-continuity programs. However, the unpredictability of the timing, nature, magnitude, and impact of a terrorist attack makes the risk much more difficult to quantify and makes risk-management significantly more challenging.

Operational Risk Management

Operational risk management (ORM) is a major piece of ERM at financial services firms and the fundamental area in which terrorism risk management must function. ORM is broadly defined to include all risks of doing business other than those considered under credit, market, and insurance areas of risk management. The key components are risk assessment and cyberterrorism.

We would expect to see two things in a business's operational risk-management plan: a sound business continuity plan and systems and procedures in place to monitor and assess terrorism risk on an ongoing basis.

Business-continuation plans are a principal piece; they are the processes and procedures companies would be using to limit the impact of a terrorist attack.

First, terrorism should be clearly identified as a potential risk in a company's business-continuity plans. Concerns covered should include crisis management, disaster recovery, and business resiliency for unexpected and severe events. We would expect to see potential risk scenarios identified, which in terrorism would include losses from direct physical attacks as well as attacks to a firm's computer systems and raids on its data. The impact of an attack on employees, customers, distributors, physical facilities, communications, data processing, and information security—as well as on records and in-process transactions—should also be considered. Finally, we would want to see the ability to explain in detail not only the current level of terrorism risk to which they are exposed but also how they would reduce the impact of a terrorist attack if there is one.

Some companies hold dry runs—surprise drills to help them assess the effectiveness and the ease of execution of their plans and how their plans work with those of local governments. One such run had an insurer's employees respond as if a surprise bomb had exploded at a street corner in the central business district very near to their offices. In the run, they traced how the bomb, were it to have exploded, would have affected both the main office and the alternate operations sites.

The alternate operations, it turned out, weren't sufficiently separate from the main operations, so operations would have been severely compromised by security and traffic restrictions from the explosion, and by local communication degradations. The company upgraded its business-continuity plan to establish more remote alternate work sites and better alternate communications.

Risk assessment

The quality of the process a firm uses to assess and monitor its exposure to terrorism risk on a regular basis is also scrutinized when evaluating ERM for terrorism risk. We would want to know what key quantitative and qualitative risk indicators the company has pinpointed, whether they are monitored regularly, and how that monitoring is done. These key indicators cover a broad range of risks, including terrorism, and incorporate inherent indicators (e.g., the number of unauthorized attempted accesses or break-ins) and controllable indicators (e.g., number of actual unauthorized security breaches). A composite indicator is simply a combination of inherent and controllable and depends on the nature of the business being assessed. They could be specific to individual business units or across the whole firm.

These measures should respond to changes in the firm and the regulatory, financial, political, physical, and insurance environment. We would view favorably a process that systematically tracks loss data from actual firm experience and from other businesses and regularly incorporates that data into the risk-assessment process.

Cyberterrorism

Cyberterrorism refers to attacks on an institution's information systems and assets via the Internet and all virtual information highways. It can involve everything from asset, information, and identity theft to viral infections meant to shut down portions of a company's information technology systems. Given the potential magnitude for disaster from a cyberterrorist attack, institutions must invest against such possibilities through well-structured enterprise-wide plans that are continuously tested and evaluated to assess the vulnerabilities and integrity.

Such a plan must clearly be developed and constructed at the enterprise level and executed using a bottom-up approach through the various lines of business, ensuring that consistency is maintained with the corporate view.

In assessing an institution's ERM practices, Standard & Poor's evaluates the level of preparedness against cyberterrorism. The evaluation looks at whether a corporate security plan is in place and if a senior executive is

responsible and accountable for developing and assessing cyberterrorist threats to the company. We also look at whether the institution tests its security plans and checks on what material issues are outstanding. In addition, we ask whether the institution has a formalized response plan, what scenarios are used to test the plan's robustness and its response function, and whether staff has been trained and educated on how to identify and be aware of such attacks.

Internal testing against cyberterrorism is necessary, but not sufficient to establish the degree of robustness of an institution's level of preparedness. Institutions should also, in our opinion, construct a vulnerability index by having external third-party cybersecurity experts validate the integrity and robustness of their security systems.

Conclusion

Five years after the Sept. 11, 2001, terrorist attacks, many financial services firms have incorporated preparing for terrorism risk into their functions. Those that have shared their plans with Standard & Poor's thus far have shown careful thinking about the contingencies. However, the constantly evolving nature of terrorism risk requires constant, ongoing vigilance, flexibility, and transformation.

Copyright © 2009, Standard & Poors, a division of The McGraw-Hill Companies, Inc. (S&P). S&P and/or its third party licensors have exclusive proprietary rights in the data or information provided herein. This data/information may only be used internally for business purposes and shall not be used for any unlawful or unauthorized purposes. Dissemination, distribution or reproduction of this data/information in any form is strictly prohibited except with the prior written permission of S&P. Because of the possibility of human or mechanical error by S&P, its affiliates or its third party licensors, S&P, its affiliates and its third party licensors do not guarantee the accuracy, adequacy, completeness or availability of any information and is not responsible for any errors or omissions or for the results obtained from the use of such information. S&P GIVES NO EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, ANY WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE OR USE. In no event shall S&P, its affiliates and its third party licensors be liable for any direct, indirect, special or consequential damages in connection with subscribers or others use of the data/information contained herein. Access to the data or information contained herein is subject to termination in the event any agreement with a third-party of information or software is terminated.

Analytic services provided by Standard & Poor's Ratings Services (Ratings Services) are the result of separate activities designed to preserve the independence and objectivity of ratings opinions. The credit ratings and observations contained herein are solely statements of opinion and not statements of fact or recommendations to purchase, hold, or sell any securities or make any other investment decisions. Accordingly, any user of the information contained herein should not rely on any credit rating or other opinion contained herein in making any investment decision. Ratings are based on information received by Ratings Services. Other divisions of Standard & Poor's may have information that is not available to Ratings Services. Standard & Poor's has established policies and procedures to maintain the confidentiality of non-public information received during the ratings process.

Ratings Services receives compensation for its ratings. Such compensation is normally paid either by the issuers of such securities or third parties participating in marketing the securities. While Standard & Poor's reserves the right to disseminate the rating, it receives no payment for doing so, except for subscriptions to its publications. Additional information about our ratings fees is available at www.standardandpoors.com/usratingsfees.

Any Passwords/user IDs issued by S&P to users are single user-dedicated and may ONLY be used by the individual to whom they have been assigned. No sharing of passwords/user IDs and no simultaneous access via the same password/user ID is permitted. To reprint, translate, or use the data or information other than as provided herein, contact Client Services, 55 Water Street, New York, NY 10041; (1)212.438.7280 or by e-mail to: research_request@standardandpoors.com.