

**Remarks**  
**By**  
**Jeffrey S. Grange**  
**Vice President**  
**Global Manager, Financial Fidelity Products**  
**Department of Financial Institutions**  
**Chubb Group of Insurance Companies**

**Before**  
**The**  
**Business Roundtable Security Task Force**

**Washington, DC.,**  
**December 13<sup>th</sup>, 2001**

Good morning.

I'm Jeff Grange, and I work in the Department of Financial Institutions at Chubb & Son, Inc. I'm am delighted to be with you today to discuss risk management. This morning, my purpose is to leave you with four basic ideas that any CEO should consider when their enterprise is confronted with a disaster that potentially could result in a major disruption to the reliability and delivery of their goods and services.

If I can leave you with one thought today: it is that our experience in the property & casualty insurance industry shows that robust, effective, and enterprise-wide risk management is the key to the long-term success and survival of your business. Seventy-five (75%) of businesses that lack a comprehensive risk management strategy prior to a catastrophic natural or man-made disaster do not recover and ultimately fail. Make no mistake risk management is a shareholder value issue and a corporate governance issue.

The events of September 11, 2001 have tragically illustrated the threat that catastrophic man-made and natural disasters pose to corporate America. September 11<sup>th</sup> has redefined everyone's conception of a "worst case scenario". Even as we grieved the loss of so many co-workers, the business continuation and contingency plans of the affected institutions kicked in and worked remarkably well.

Think about it. Our infrastructure held.

As with any catastrophic event, this tragedy has heightened awareness of the importance of operational risk management. Operational Risks, unlike credit or market risks are exceptionally diverse and broad. For those infrequent and uncontrollable catastrophic events such as the World Trade Center tragedy a comprehensive risk management plan plays a crucial role in the survival and recovery of the enterprise.

The property and casualty insurance and reinsurance industry can provide practical risk management guidance on disaster recovery risk management and demonstrate how insurance can be used to finance and transfer the financial risks of low frequency, high severity catastrophic losses.

Companies can survive tragedies like the World Trade Center if they engage in comprehensive planning and preparation for a full range of disasters. By “comprehensive,” I mean planning risk management in the immediate, intermediate, and long terms – all three.

For example, many of those financial services and other firms that were located in the World Trade Center continue to function because they had comprehensive, up-to-date backup and contingency plans that have been implemented. Many of those companies also were policyholders with insurers who made advance payments on claims. The advance claims payments provided immediate funding to cover the costs of implementation for these disaster recovery plans.

Hopefully none of us will ever have to face another terrorist attack. However, financial services firms have always been subject to both natural and man-made disasters -- such as hurricanes, floods, snowstorms, fire, chemical spills, riots, and more - that could potentially interrupt normal business operations.

My experience has been that companies that survive with a minimum of damage have done comprehensive planning and preparations. They have well-tested contingency plans that address a full range of different kinds of disasters.

At the outset I indicated that I have four specific recommendations that each of your CEOs should address, but first would like to offer two specific recommendations for your working groups this afternoon.

First, I would encourage you to consider a recommendation that explores core corporate governance principles in the aftermath of September 11. In short, how has September 11 really affected core business operations and principles? Other than focusing on emerging threats and security, what is it about the attacks that affects our companies, our core business operations and shareholder value? I would ask your working group to consider a recommendation on reporting lines, accountability and responsibility from senior management to the board of directors as respects enterprise risk management and business continuation planning.

Second, based on these corporate governance inquiries, what new programs and processes should to be considered and how should these initiatives emerge? One options being considered down the street from here is through legislation and regulation. Already Congress and the agencies are looking at quick fixes. In the alternative, perhaps the Business Roundtable will consider a formal program for engaging the auditing community so that enhanced security inquiries become part of every CEO agenda, the Audit Committees review, and an outside auditor's checklist of items.

My experience has been that companies that survive with a minimum of damage have done comprehensive planning and preparations. They have well-tested contingency plans that address a full range of different kinds of disasters.

An effective contingency plan should be based on the assumption that the company does not continue operations at its principal physical location due to natural disaster or some other unforeseen event.

And that plan should be tested annually, at least. Some large firms that had offices in the World Trade Center found their computer systems disrupted nationwide for days. That's because their servers were in one of the towers and their backup systems wouldn't come on line.

Of course, no contingency plan on earth can replace the people who deal with your customers and operate your systems. The tragic loss of life suffered by many companies at Ground Zero on September 11 underscores the need for all employees to be familiar with the company's contingency plan.

I'd like to stress that I am talking about contingency plans for the entire enterprise, not just IT operations. And those plans should be updated as systems and circumstances change. That's the best way to manage immediate risk.

I indicated at the outset that I would focus on four key points that every CEO needs to know when dealing with disasters. They are:

1. Anticipate worst-case scenarios
2. Test, test, test your disaster recovery plans
3. Maintain communication with all employees
4. Establish clear lines of authority, responsibility and accountability

1. A comprehensive disaster recovery plan must include plans to secure off-site office space for key employees. One major Wall Street brokerage firm's version of a disaster recovery plan has been to rent out an entire mid-town hotel. Another major bank had an off-site back up premise but it was so close to the primary facilities that it was also disrupted by the World Trade Center event. It is vital that an effective disaster recovery plan has a site that is supported by a secondary power grid and secondary telephone switching location.

One lesson learned from World Trade was the importance have having an available supply of desktop computers, laptops, servers and office furniture in an alternate location so that key employees can actually get back to work quickly.

2. It is absolutely vital that the organization test, test, and test again their disaster recovery plans. You have a plan, but you need to make sure it works when you need it to. If you don't test the best business continuation plans in the world are useless. Property & casualty insurers have loss control specialists and disaster recovery consultants on staff that can assist companies with the design, implementation and regular testing of business continuation plans. Companies should live-test one worst case scenario at least once a year. A large Canadian bank six months ago live-tested a bio-terrorism incident that took place at its principal headquarters location in Toronto. In light of the ongoing anthrax contamination threat this scenario testing is an example of real foresight.

3. It is vital to the recovery and survival of your company to maintain constant, clear, communication with all of your employees at a time of crisis. I cannot tell you the number of companies affected by World Trade Center who did not even have simple employee contact telephone trees. Helping your employees –your key organizational

asset- cope with the impact of a disaster is your first priority.

Communication is essential to begin the process of re-engagement, the implementation of the disaster recover plans and recovering the business. You need to know where your people are following a disaster, identify what they need and direct them as to what to do.

4. CEOs need to establish clear lines of authority, responsibility and accountability for disaster recovery. What happens if the board and senior management of the organization are killed, missing, incapacitated or inaccessible. The first seventy-two hours after a disaster are vital for the long-term survival of the enterprise. Having a temporary chain of command and ensuring that the leadership capacity and decision making models of your organization are “hardened” and remain viable post disaster will oftentimes make the difference between the organization recovering or not.

Property & casualty insurers stand ready to work together with the insurance risk managers and business continuation planners at your organizations on each of these four key ideas.

What about risk management in the longer term?

Well, the transformation to a digital world is altering both the nature of risk and its impact. Our growing reliance on technologies, particularly Internet technologies, exposes companies to the risk – that the technologies are disrupted and criminals misuse them.

We've always understood that these networks are one of the battlegrounds on which terrorists will engage us. But now we understand just how much damage these terrorists are prepared to do.

We need to do whatever it takes to stay on top of security and our vendor relationships. We must protect that part of the critical infrastructure, because as companies increase their dependence on new technologies, the consequences of an interruption of these services can become quite severe.

CEOs must be prepared to ask and answer the question: Is your company prepared for cyber attacks, cyber terrorism, and information warfare? The technological advance into cyberspace does not come without substantial risk. The more dependent a company becomes on the Internet and electronic communications for their service offering the greater the potential vulnerability and exposure to wide-scale service disruption.

Information security should be a priority for every CEO, corporate officer and company director as well as the company's insurance decision makers or risk managers.

Information security is core to brand reputation. Information security is a line of business issue, it is no longer an "IT" issue. Information security is a core competency and is "mission critical" for most enterprises going forward. Ultimately the board of directors are accountable for the governance of the corporation and cyber risks can significantly affect shareholder value, corporate stability, reputation, brand and financial performance. This vulnerability requires an organizational commitment to build the processes to protect and secure critical information in the fast moving, fully networked environment that global connectivity has created.

As the enterprise migrates more and more of its traditional core business processes to the web, more and more valuable corporate information and data is made available to employees, customers, vendors and partners. The value of such intangible property or data has increased exponentially in recent years while access to this highly valuable proprietary data is virtually unfettered. Anyone with access to a web browser application and the Internet is potentially a user of your systems and your confidential and proprietary intellectual property.

In the wired world the threat of cyber-crime is very real. Any computer or network can be hacked by anyone, at anytime from anyplace in the world. When it comes to critical infrastructure security experts have said that it is child's play for serious hackers & crackers to wreak havoc and disrupt corporate and government networks. It may be possible for a well-planned attack to paralyze communications, financial and transportation systems. The critical telecommunications and computing infrastructure backbones upon which we increasingly depend are extraordinarily vulnerable to CyberAttack.

I'd like to close by hi-lighting the importance of leadership and corporate governance that is required of all us to confront both traditional and emerging threats. The tragic events of September 11 are a defining moment for us all. As business leaders we are going to be dealing with the consequences for years, on a variety of different levels.

However, investing huge sums of money in information security systems alone will not solve the problem of cyber attacks. Beginning at the highest board and management levels, companies must become educated about the risks of the digital world.

No company is 100% secure and immune from these on-line menaces and cyber criminals. Responding to these cyber threats requires an enterprise-wide commitment and strong risk management policies and procedures established at the top of the corporate ladder. This board level commitment must bridge the gap between IT and risk management in the organization. Ensuring that information security becomes a line of business issue will go a long way to protect the company assets and officers from the pending threat of cyber-criminals.

Thank you.

Filename: Business Roundtable Remarks on Risk Management  
and DRP Planning DCO Version 3.0 12 13 01 J Grange.doc  
Directory: F:\CDROM  
Template: C:\Documents and Settings\Administrator\Application  
Data\Microsoft\Templates\Normal.dot  
Title: Good afternoon  
Subject:  
Author: FDIC  
Keywords:  
Comments:  
Creation Date: 1/30/2002 8:53 AM  
Change Number: 2  
Last Saved On: 1/30/2002 8:53 AM  
Last Saved By: Jeffrey S. Grange  
Total Editing Time: 0 Minutes  
Last Printed On: 4/9/2002 3:40 PM  
As of Last Complete Printing  
Number of Pages: 13  
Number of Words: 2,032 (approx.)  
Number of Characters: 11,583 (approx.)