PRICEWATERHOUSECOOPERS

Investment Management Lyceum Forum Highlights

Risk Management: Crisis Management and Third-Party Relationships

Moderator:

Barry Benjamin
Partner, Investment Management, Assurance and Business Advisory Services
PricewaterhouseCoopers

Speakers:

Thomas Barrett
Partner, Investment Management, Global Risk Management Services
PricewaterhouseCoopers

Rich Carson
Partner, Investment Management, Assurance and Business Advisory Services
PricewaterhouseCoopers

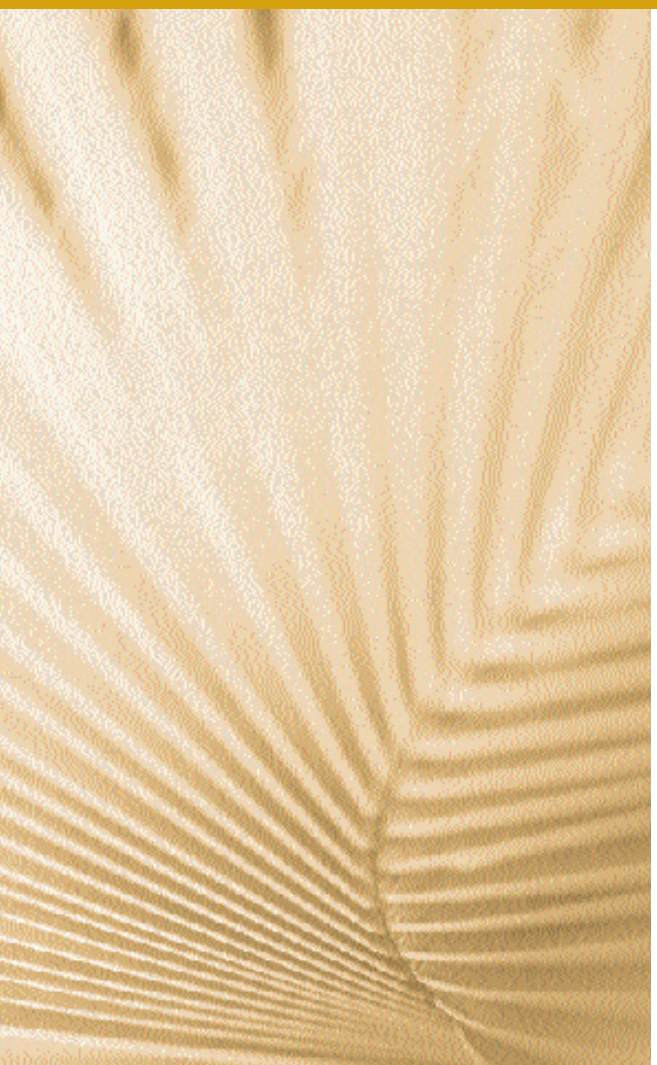
Panelists:

Randolph Brock
Executive Vice President, Risk Oversight
Fidelity Investments

Linda Kim
Managing Director and Chief Operating Officer, U.S. Index Management
Barclays Global Investors

Frank Principe
Senior Director of Operations
FT Interactive Data

Mark Vandehey
Vice President and Director of Internal Audit
OppenheimerFunds, Inc.



Preparing for the Unthinkable

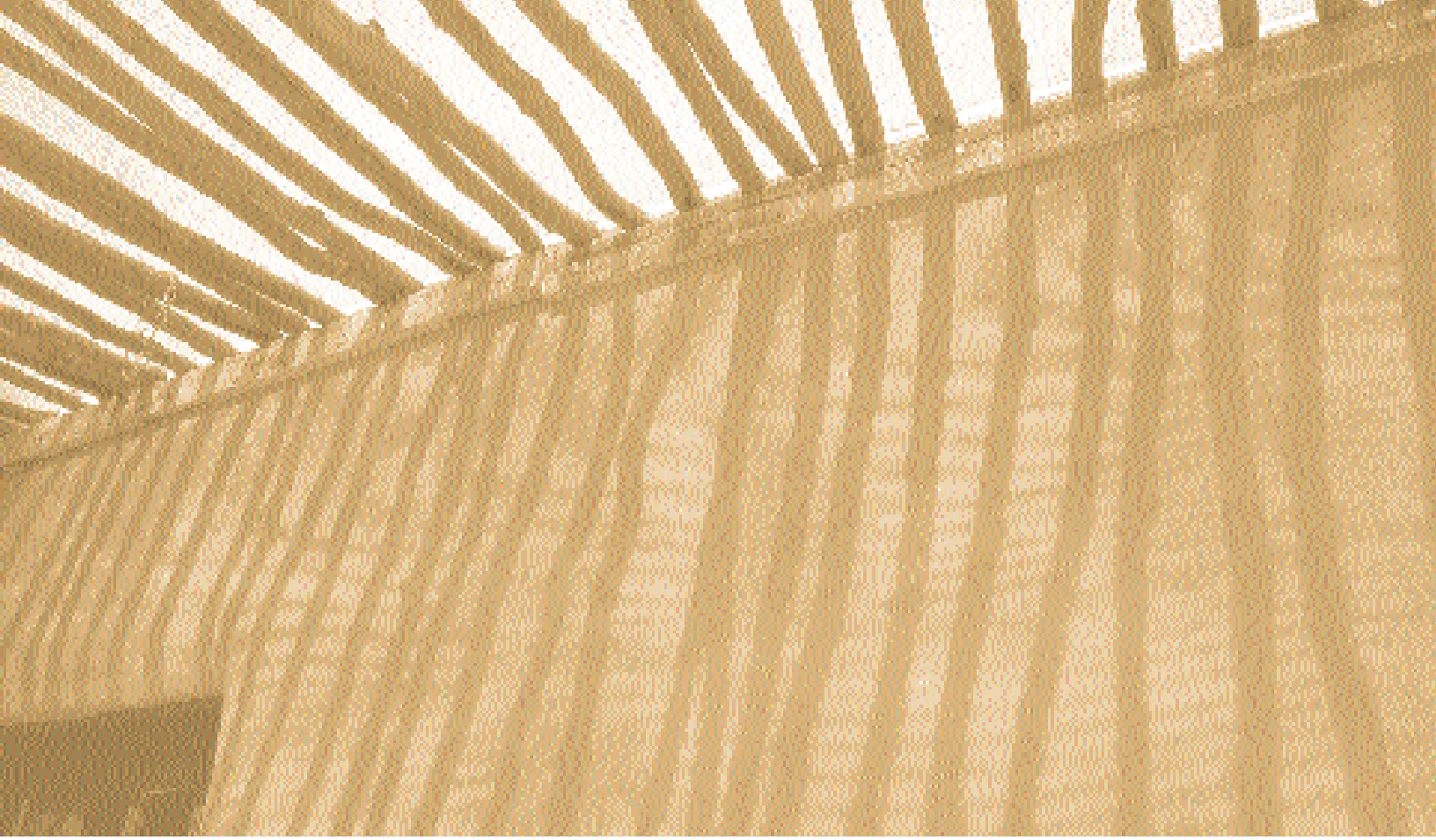
Managing Risks in the Event of a Crisis; Minimizing Risks in Provider Relationships

The tragedy of September 11 brought the subjects of risk management and disaster recovery front and center for thousands of companies and millions of people, and the focus of the public's interest was probably greater on the financial services industry than on any other. Fortunately, it appears, the investment management industry performed well.

But in the aftermath of the tragedy, even firms with the most sophisticated risk management functions recognized that they had more to learn and much to do in preparing for a crisis in their own operations and monitoring how well their key service providers could perform in a crisis of their own. Many other companies, those that have paid less attention to these matters, suddenly recognized how vulnerable they are.

To help foster a dialog on these elements of risk management, PricewaterhouseCoopers conducted a Lyceum Series Forum for the investment management community. The forum was held in Boston on December 5, 2001. The session was videotaped and is available for viewing until April 5, 2002, at http://webevents.broadcast.com/pwc/lyceumforum1201.

❖



Crisis Management

Research shows Financial Services Industry is Poorly Prepared for Disaster

The investment management industry performed quite well on September 11, despite the fact that research shows the financial services industry is poorly prepared to deal with crises, said Rich Carson, partner at PricewaterhouseCoopers who specializes in the investment management industry.

Carson said that industry studies indicated that as many as 85% of financial services companies have a disaster recovery plan, but only about 10% to 15% have a fully conceived risk management plan.

Disaster recovery, he said, is "focused solely on the key systems and key connections inside and outside the company that would need to be brought back in the event of a crisis." Thus, disaster recovery is only an element in a crisis management plan, which in itself should grow out of a broad risk management strategy.

Firms Face Undefined Risks

"Relatively few financial services companies have dealt with their business risk profile in a wall-to-wall manner, assessing the full range of risk their organizations face, identifying what risks they want to mitigate and how they should respond. As a result, they are leaving major business continuity risks unaddressed," Carson said.

"Very few have established a crisis management team and a response plan," he continued. "This suggests that a good number of companies are taking considerable risk by not having defined plans, roles, responsibilities and testing procedures to make sure they are ready to respond to a crisis."

Are You Prepared?

CRISIS: *A crucial or decisive point; an unstable state with impending abrupt change; sudden change for better or worse; disaster, catastrophe, calamity, emergency.*

CRISIS MANAGEMENT: *A process based on planning that uses training, skill and instinct to protect an organization's assets, people, public image, business relationships and business continuity and to minimize financial loss.*

Effective crisis management is accomplished through prompt response, early and continuous communication and effective execution. Success typically depends upon formal and informal actions growing out of a well-conceived action plan backed by an organizational structure specifically developed to manage crises.

— Rich Carson, partner, PricewaterhouseCoopers

A company's basic character, "all its strengths and flaws," are exposed to the world when a crisis occurs, Carson said, and ineffective response and poor communication can deeply harm the confidence of clients, employees, business partners and regulators. Even if the response is effective and the communications poor, great damage can occur.

"Effective crisis management requires rapid decision-making in an atmosphere of great stress and human emotion," Carson said. "The odds favor failure, not success—all the more reason for planning and testing."

The events of September 11 have served to remind the investment management industry of the risks of losses and business interruption, Carson said, but other forces are also encouraging managers to take a new look at crisis management and business continuity plans. These forces include a wave of new mandates from regulators, increased reliance on service providers, greater management awareness of the risk-management process, growing concern about insurance renewals and the mounting belief in board rooms that prudent management requires that more attention be paid to enterprise-wide risks.

Six Key Risks

Carson described the key risks facing a firm in the event of a crisis—risks faced even by those companies with a crisis management plan:

- ***An unclear action plan,*** which can lead to poor communications and may inhibit prompt action—because people are confused about what they should be doing.
- ***Loss of control of the organization,*** potentially increasing the size of financial loss.
- ***Loss of confidence in the organization*** by clients, employees and others.
- ***Inability to locate key people,*** including service providers, leading to a breakdown in systems, telecommunications and transportation as well as a general inability to act.
- ***Hasty or disorganized resumption of business***, which threatens the accuracy and completeness of all business activities.
- ***Inability to source critical data from service providers*** because they were unprepared for the crisis.

It's impossible to plan for every eventuality, Carson stressed, because crises are by nature unpredictable—and so are human beings. "A major event would involve a lot of people, and you never know how they might react." For example, he described testing situations in which it had been discovered that key individuals had moved without providing new phone numbers, with the result that the company's response was ineffective.

Carson traced the steps in developing an effective crisis management plan:

1) Develop a conceptual business continuity framework.

This involves "looking clearly at what is required in terms of systems, resources and skills to recover from a crisis and continue operating." This also involves analysis of existing and potential back-up systems, the involvement of service providers and the operating history of the company itself. "You need to ask what crises have occurred in the past and how effectively you dealt with them," Carson said.

Crisis Management Team

Throughout his presentation, Carson stressed the importance of individuals in making a crisis plan work. "In a true crisis, it will be the people designated to serve on the crisis management team who will be crucial to the success of the recovery plan."

The team, he said, should have the following major roles:

- *Providing immediate and ongoing support to employees and their loved ones, those personally affected by the crisis and those charged with bringing back operations.*
- *Immediately assessing the impact of the event and declaring the nature of the crisis.*
- *Keeping all important parties informed on the status of the crisis, the actions being taken and the progress being achieved.*

Carson proposed the following lineup for an effective crisis management team: chief executive, human resources officer, risk management officer, community/public relations officer, chief technology officer, legal representative, facilities manager, leaders of business units.

Crisis Management continued from page 3

2) Establish priorities.
"You have to establish priorities about which systems or processes you want to bring back first and in what sequence. You can't just say you want to bring the entire business back, because that may not be the right answer." Priorities must also be established in terms of use of facilities, and a chain of command decided upon. "Someone needs to take charge and that person must be identified so that he or she comes to the front of the class as soon as possible."

3) Design a response plan.
The plan should include such elements as management roles and responsibilities, management's access to critical information and communications actions that will be taken to inform key internal and external audiences. A crisis management command center must be established, and a process put in place to gather information for future evaluation. "Someone has to be able to make the call on the level of the crisis and the level of response," Carson said. "Once you get an idea of what's going on, communication must begin right away and must continue constantly. Your updates should show that the management team is at work, that a response is under way. A lot of people are wondering if your company is going to survive."

4) Align the plan with the organization.
A plan can't be developed in a vacuum; it must relate to the firm's people and structure. This raises the possibility of cross training and knowledge sharing among various departments, as well as the development of alternative processes and alternative sources of data.

5) Test the plan periodically.
Live tests are rare events, but can be quite valuable, Carson said, uncovering unexpected problems that must be fixed. New crisis scenarios, some of them extreme, should be explored in light of the plan. Various "small, day-to-day crises" allow for testing of parts of the plan. Service providers should be tested or examined to see if they can really do what they say. "You need to exercise your plan. It's not a book you put in a drawer because frankly you may not be able to find the book when you need it."

6) Re-evaluate and redesign the plan.
Only a plan that has been kept fresh can be effective. It must be updated to reflect new operating circumstances, business relationships and major events that have affected the company. "An outdated plan is useless. You won't be able to plan for every event, but continual preparation means you'll be able to respond better when you have to." ❖

Crisis Management

After September 11: Lessons from the Real World

Moderated by Barry Benjamin of PricewaterhouseCoopers, *a group of executives responsible for risk management in their organizations discussed how the attacks of September 11 affected their companies. Their remarks are summarized here.*

Benjamin: How has your world changed since September 11?

Mark Vandehey, OppenheimerFunds: The big change for us is that crisis management has everybody's attention now. We had 600 people in the World Trade Center. They all survived. Fortunately, we also had a plan that was overseen from our operation in Denver. Overall, we are pretty comfortable with the way we recovered, but we are rethinking some issues. In internal communications, we did not anticipate the difficulty we would have finding all of our people; we've now established a Web site for that purpose. We also didn't anticipate the loss of commercial airline service to move back-up data tapes and other crucial materials. We were able to use a private air service to help us.

Linda Kim, Barclays Global Investors: With headquarters in San Francisco, we always thought of a major disaster being an earthquake. Our focus has been on assuring continuity of operations. We have our data center in Sacramento, 100 miles from San Francisco, outside the earthquake zone. It sits on two different power grids in case one goes down, as well as a generator backup. We have quite an involved plan, and PricewaterhouseCoopers helped us evolve it further back in 1995.

What really affected us on September 11 was the impact on the whole industry and on third-party providers. We had done due diligence and our top-tier service providers came through pretty well. But we realize we must expand the way we look at service providers to include our counter-parties' providers, because there's a sequential knock-on effect that is our weakest point. I think the whole industry felt it. So for us, the emphasis is looking at the whole chain of service, not just the immediate circle.

Randolph Brock, Fidelity Investments: We think our plans worked very well, but September 11 showed us that there are some things we can do better. It also expanded our knowledge of the universe of potential risks that could affect us. So we have undertaken a strategic reassessment of the way we look at business continuity planning. For one thing, we've made some organizational changes that have already helped our planning.

In terms of expanding our thinking, we believe that in the past we placed too much emphasis on infrastructure and not enough on people. We can insure that we have alternate sites with systems that can be switched over, but if we lose people, as some of the businesses in the World Trade Center did, we are in trouble. If the people who perform the critical functions are lost or incapacitated, the fact that we have an infrastructure capable of being switched over is meaningless. So we are refocusing on that situation now.

Frank Principe, FT Interactive Data: (FT Interactive Data is a leading provider of financial information and analytical software to global markets.) Well, from our side, there is a crisis every day. We review and adjust our crisis management plan semi-annually. Our plan worked on September 11. We are proud that we were able to meet our delivery requirements. However, there are changes we are making. Our major New York location was only a few blocks from were the tragedy happened. We had back-up sites in other locations. But now we want to establish two live sites in New York and have them back up each other. We also want to improve the functioning of the back-ups we have in place.

Benjamin: Any other thoughts on the impact on people? Their willingness to move temporarily to other cities to do contingency work, for example?

Crisis Management *continued from page 5*

Kim: Continuity rather than resumption is our fucus. I live in an earthquake fault zone. If one hit my house, I don't know that I would be up for going 100 miles away to Sacramento. That's why we have critical functions represented in both San Francisco and Sacramento—traders, portfolio managers. And we do business unit testing to make sure that if one location goes down the other can pick up immediate needs. So people are available every day in their own home areas and we are less likely to be affected by a regional disaster.

***Benjamin:** Mark, on September 11 the cellular phone system in lower Manhattan went down. How did you deal with that?*

Vandehey: Immediately, many folks left Manhattan island and were able to call in. We have a toll free "emergency line" that we used for the disaster in New York. People were able to call in, get recorded messages and report that they were o.k. They were also able to use e-mail. It took about 24 hours to locate everyone.

But we were up and in a crisis management mode very quickly because the ten or so people that you really need to talk to had cell phones. We have key numbers posted on a Web site; and each manager has a folder with critical phone numbers. We set up a conference call service in Denver that allowed managers to call in for scheduled meetings. So it went smoother than we might have expected.

***Benjamin:** Do you feel that effective crisis management can be promoted as a competitive advantage, that you could educate people about how reliable your plan or system is? Do you see it becoming something that would be more important to report to shareholders and customers?*

Principe: To us, yes, we think it definitely is an advantage. We were commended by many clients on our communications efforts with them. We use our Web site, fax broadcasts, verbal contact. We are pleased when clients want to come and sit down with us and look at our plans.

Brock: The best communication comes in the aftermath of a disaster when a business has in fact recovered and everyone can see it. Post September 11th, people saw

that Fidelity had prices in the newspaper on the first day it was possible, when many competitors had "NAs" for prices. That's the best proof in my opinion.

Kim: Good crisis management is not so much a competitive advantage as a bare necessity. I think clients expect that you have plans in place, that they're tested and that you can continue your business.

Vandehey: I agree. We were functional within four hours of the disaster and were trading on the bond market the next day. Having the functions working and getting out that message were the most critical things for us.

Benjamin. Even with September 11, I sense a reluctance in some companies to conduct tests. How do you get the operating units to be more enthusiastic about the importance of testing rather than just thinking it all through?

Kim: Testing is absolutely critical. The way to get the organization aligned in favor is to set the tone at the top, having your chairman say that it will be done. In fact, we do annual simulations. We relocated close to 100 people in a simulation in the past year. Everything may look good on paper, but when you get into a simulation you learn something every time. We have designated leaders from various groups and we run through the drill.

We have the firm-wide tests and tests in the business units for their specific systems, people and processes.

Vandehey: We've never done an enterprise-wide simulation of a crisis. We do small simulations. We've been doing it for 20 years or more. We test our technology. We make sure that the user community is involved in each of the technology tests. We had a trading floor recovery test in New York in August, just before the attack.

I agree that if the people at the top push for tests, it's going to happen. For us, the 1993 bombing of the World Trade Center was an important wake-up call. It was minor compared to what happened this time, but it got people really thinking about what was needed and it paid off.

Principe: We do small simulations, but it's something we are thinking about changing. Because we have to deliver every day, we go through our process and look at the areas we believe have the most risks, and that determines how much testing we will do. We have used our success on September 11 to stress internally how high our standards are and how we have to keep working to maintain them.

Brock: Profit is not the responsibility of the profit department and business continuity is not the responsibility of the business continuity group. It's the responsibility of management. So it has to be a philosophy that permeates the organization. Our chief operating officer has described himself before large groups as the chief risk officer. We've instituted a contingency process by which plans are in place, tested and measured for each business unit—and then reported to the the audit committee.

We need to do more in terms of connecting the tests of the individual business units to the enterprise-wide test, making sure the linkages are effective and really do work. That's something we'll be paying a lot of attention to next year. ❖

Third-Party Management

Technology Boom Raises Big Question: Who's Watching the Service Providers?

Increased reliance over the years by investment management companies on third-party service providers has given rise to growing concerns about the dependability of those providers, especially in times of a crisis, said Thomas Barrett, Investment Management Partner in global risk management services at PricewaterhouseCoopers.

Many of these providers have assumed roles that in themselves have grown in importance as the Internet has flourished as a place of business, he pointed out.

"The investment management industry has long used third parties for such traditional roles as fund administrators, custodians and transfer agents," he said. "But as reliance on technology has grown and because resources are scarce, we've seen new alliances take shape in which third parties are used to host Web sites, manage content on those sites and deliver prospectuses."

These Web sites have turned into important processing and information centers, operating around the clock. The customer makes no distinction between a company and its service provider. If either one fails, it's a black mark against the company's reputation. A classic example of this occurred, Barrett said, when a financial services company discovered its Web site had been located by a third party on the same server as the FBI—with the result that it was constantly crashing as the FBI came under attack by hackers.

Outsourcing by Outsources

To make matters even more confusing, Barrett continued, third-parties often outsource some of the work to yet other providers, creating tiered relationships that remove control even farther from the sponsoring company.

"When you combine constantly changing relationships with constantly changing technology with constantly increasing reliance on technology, things can spin out of control pretty quickly," Barrett said.

As a result, many companies are re-evaluating the way they manage risk in their third-party relationships. This re-examination is also occurring because of the bursting of the dot.com bubble, major public difficulties suffered by high-profile companies that fell victim to hackers, viruses and melt-downs. Increased regulatory concern over the role of service providers is also a factor.

"We are finding that some third parties don't sufficiently understand the importance of the fiduciary responsibilities that are inherent in financial services or the regulatory requirements that govern our client relationships. We may be delegating too much authority to them and to the companies they are partnering with," Barrett said.

Investment management companies generally have done a good job in the basic steps of outsourcing, he added, such as determining which functions to turn over to others, in choosing good partners and in writing effective contracts governing the financial arrangement. However, far fewer have effective monitoring programs and fewer still conduct on-site reviews. They also have paid too little attention to developing an exit strategy if things go wrong.

Ten Important Questions

Barrett listed these questions a company should answer to help determine its exposure to risks from the activities of third parties.

- ***Does your operational risk-management program include provisions for monitoring third-party providers or strategic partners?*** In some companies, the subject is not even addressed as a potential risk.
- ***Have you considered the feasibility of being able to manage third-party relationships?*** "You may not be capable of doing it under your current risk-management organization," Barrett said. "Many large companies have multiple relationships—many different management points—with the same third party."
- ***Have you considered how critical the outsourced function is?*** "You need to establish priorities for these activities based on the damage that could be caused to the company or its reputation if the function goes down."
- ***Have all important measurements of effectiveness been included in the contract?*** "The contract often doesn't include financial and control metrics that help a company gauge how effectively the service is being performed. Periodic reports or reviews would be helpful. "
- ***What are the communication and escalation processes in the event of a crisis?*** "What kinds of events need to be reported and to whom? What are the contact points between the two entities?"
- ***Who is responsible for monitoring third-party relationships?*** "Once the due diligence is done, after the contract is signed, it's not always clear which people own the relationship and are responsible for it on a daily basis."
- ***Are monitoring controls strong enough to detect potential problems as they occur?*** "We've found that many monitoring arrangements operate after the fact, reporting problems that occurred in the past. It's more important to have a system that warns you as some sort of erosion begins taking place."
- ***Is the decision to exit defined?*** "You need to think about what kinds of circumstances would cause you to end the arrangement."
- ***Are there workable arrangements regarding the transfer or destruction of the data if the arrangement is terminated?*** "You must be certain that you retain ownership of the data and that you are able to ascertain to your complete satisfaction that it has been destroyed or transferred entirely to the new agent."
- ***Does the contract contain specific clauses that deal with exiting?*** "You need to be sure all the important provisions for getting out of this arrangement are workable."

"I hope it's clear from all that I said that monitoring third-party providers is an ongoing management process that has to continue from day one," Barrett concluded. "The whole area is changing so rapidly that no other approach will succeed." ❖

Third-Party Relationships

Lessons from the Real World

Here are summaries of the panel discussion that followed Thomas Barrett's presentation.

Barry Benjamin, PricewaterhouseCoopers: Frank, as a service provider, how do you look at third-party risk?

Frank Principe, FT Interactive Data: As you know, we are both a vendor and a client. We monitor our vendors and their quality very closely. We manage these relationships daily, first by the functional groups that are responsible for the relationship and second by cross-functional teams responsible for risk management. We are in constant communication with our clients, making sure there are redundancies in place and that they are satisfied with the timeliness and quality of our service. So managing the relationship is ongoing, and it keeps changing as the client's needs change.

Randolph Brock, Fidelity: You've emphasized that this is a continuous process. But I believe the key is on the front end, when the due diligence is done. The easiest way to prevent a troubled relationship is not to enter it in the first place. So it's important before the fact to look at the site, test the security, interview the principals and examine the company's history, particularly its tendency toward litigation. The worst thing in the world is to become involved with a company that likes to sue its business partners.

Beyond that, there is still a need to continuously examine technical, business, security and integrity issues involved in the relationship. And there must be a process in place to see that it in fact happens, that somebody is responsible for ongoing monitoring and due diligence. I'm not saying we do this perfectly; we need to do more to make ongoing due diligence as effective as front-end due diligence.

Rich Carson, PricewaterhouseCoopers: I wonder how many organizations really test their third-party providers. Certainly there is a lot of discussion back and forth, but to what degree are deep, periodic evaluations made? We need to understand how well they can perform not only on a day-to-day basis but also in the event of a crisis, how they would recover and how the client company can recover if the third-party can't. To really understand that, you need careful, in-depth simulations.

Linda Kim, Barclays Global Investors: You have to manage the relationships throughout the organization on a spectrum, with monitoring at a higher level where the risks are higher. There is also intensive daily monitoring and review of various operating and technology functions. If issues appear to be developing with service providers that affect key areas of the company, we will look in depth at their capabilities. Having said that, whatever you do, it never feels like it's enough.

Mark Vandehey, OppenheimerFunds: If you have a daily relationship with a key vendor, you are always pushing them to perform at the top level. There are plenty of little minor glitches that give you a sense of how they are going to perform in a more significant crisis. This gives you many opportunities to assess vendors and make contingency plans. If that means changing vendors, fine, but most want to keep you as a client and will work with you to solve potential problems.

***Benjamin:** Clients are generally looking for the same kind of information from the newer vendors who specialize in E-commerce. So it makes us wonder if there is an opportunity to retain an independent, trusted party to come in and conduct tests so that each client would not have to do it individually. I'm thinking of something like the SAS 70 types of reports. Would that be useful?*

Vandehey: We do require SAS 70 reports, or their equivalent, from several of our key vendors. We also conduct on-site visits at the start of a relationship and as it continues. I'm not sure you can get to where you want to be by simply reviewing the metrics a vendor gives you. That picture is always going to appear a little rosier than it really is.

Brock: September 11 was a significant test of whether a vendor's plans worked or not. Some worked well, others didn't. In one case, we found that a key vendor was not candid about what was working and what wasn't. We've sent cross-disciplinary teams out to visit certain key vendors with a real focus on their business continuity plans and planning processes to satisfy ourselves they were what was represented. We learned a great deal, including some lessons about ways to improve our own processes.

Regarding common tests or standards for financial services, we were visited the other day by a large accounting firm proposing a sort of ISO 9000 for financial services firms so there could be an independent test of quality. It's an interesting concept; I don't know if it will take root or not.

Kim: We do have monitoring capabilities in the more traditional sections of the business, such as pricing vendors. Our technology group uses ISO 9000 for some of its vendors. I like the idea of an industry standard for these newer areas.

Principe. On the subject of metrics, we obviously measure ourselves on the quality of what we deliver. Our clients are measuring us on our ability to meet our commitments and maintain standards of service. Beyond that, we measure ourselves on about 40 measuring points every day. Our goal is always to be sure that there is some kind of workable alternative in place.

Thomas Barrett, PricewaterhouseCoopers: Returning to the subject of on-site visits, it seems that few companies embrace the idea of going in and kicking the tires and getting the tone of the organization. I'm curious about the extent and nature of these visits in your organizations.

Kim: With key vendors its almost a daily event because there's a partnership type of relationship. Kicking the tires is really the best way to find out what's really going on.

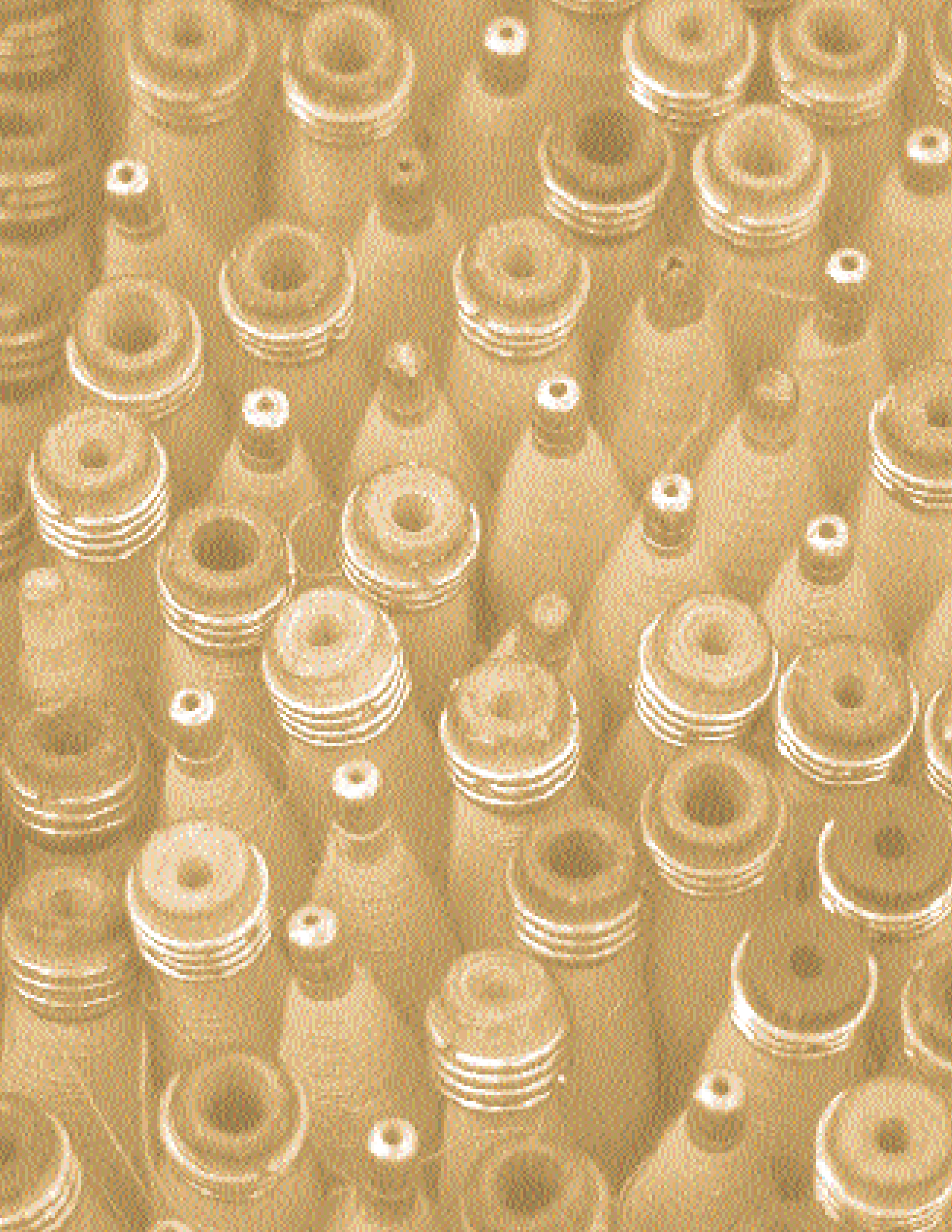
Vandehey: I agree. For critical functions it's almost a daily thing. Every banking vendor we have considers themselves being tested to keep the relationship alive.

Principe: We often visit our clients. We show them the results of our measurements, which includes times we have fallen short. Generally this is very helpful in explaining to our client base what we are doing to ensure reliability. At the same time, it improves our understanding of how clients use our data and what they expect from us. And this in turn helps us set priorities for areas that need improvement. I think these activities are critical to our business.

***Benjamin:** We're seeing situations now where instead of having software in house and on site, companies are trying to get it off their systems and go towards a service-provider approach. What kinds of changes do you see going on there?*

Vandehey: We haven't done much outsourcing. We have all our critical systems under our own control. There's a certain nervousness about going outside with critical systems.

Kim: I agree. We work to strike a balance between insource and outsourcing systems. You want to be able to have control over critical applications. ❖



Crisis Management

Audience Questions and Answers

A lively interchange with the audience developed at the end of the forum. Here are summaries of some of the questions and answers.

Q. Following September 11, are any of you defining crisis differently than you did before?

Randolph Brock, Fidelity: We have three levels of crisis, September 11 being the first level and levels two and three being less serious. September 11 was not just a one-day crisis. Since then, we've had about 130 mini-crises, from suspected Anthrax to bomb scares, to all the normal but heightened things that happen after a major crisis.

Linda Kim, Barclays: We are also looking at various levels of response, asking, in effect, "At what level of crisis do we engage what level of response?" But we need to look more at how our business is impacted by industry-wide events.

Q. The subject of crisis counselling has become very prominent in the wake of September 11. I noted that it extended to people who were not directly affected by the crisis and also weren't involved in recovery efforts. They were stuck at home with CNN and some of them felt they weren't part of their company anymore.

Rich Carson, PricewaterhouseCoopers: That's an interesting point. I happened to be at an audit committee meeting with a client on September 11. We deferred the meeting and watched CNN for about an hour and a half. Some of the faces in the room were empty. They were lost, drained of purpose, I thought. It crossed my mind that they might be on some company's crisis management team and I'm not sure they could have acted. The lesson is that we must pay a great deal of attention to the human side of things.

Mark Vandehey, OppenheimerFunds: We took full advantage of crisis counselling services starting within 24 hours of the event. We have relationships with counselling firms as part of our employee benefits package. We had individual and group counselling available to people who were directly involved in New York as well as those in Denver. The group sessions turned out to be very valuable in allowing some people who were not directly involved to get together and share their experiences.

Barry Benjamin, PricewaterhouseCoopers: One observation we hear repeatedly is that counselling may be necessary well after the event, perhaps six months later when an aftershock hits. You have to build that eventuality into your plans, because it's going to affect people and their productivity down the road.

Q. Are your companies doing anything differently in terms of funding your business recovery or continuity department since September 11? Are you getting bigger budgets or additional resources?

Vandehey: Everybody is paying a lot more attention to it, and I expect that if we need money for the changes we anticipate making, we'll find it somewhere. But there hasn't been any block grant from senior management, if that's what you're asking.

Carson: Several clients have talked about revisiting the plan and going through it as a group to see if how it might be refocused and new priorities set. At the time of the crisis they didn't open the folder and look at the plan; they reacted based on their training.

Kim: We once had a recovery folder five inches thick that people were not going to open. We cut it down to bullet points and checklists, but it is still tough reading. So much of this is experiential. That's why we have new alternates from time to time to back up the senior primary leaders. You look at the whole process very differently when you are in the hot seat and have to deal with a crisis minute by minute. ❖

Best Route to Answers

Is Through Shared Knowledge

"It's obvious from our discussions today—and certainly an understatement—that those of us in risk management are dealing with a challenging mix of issues and forces," said Thomas Barrett of PricewaterhouseCoopers in closing the forum.

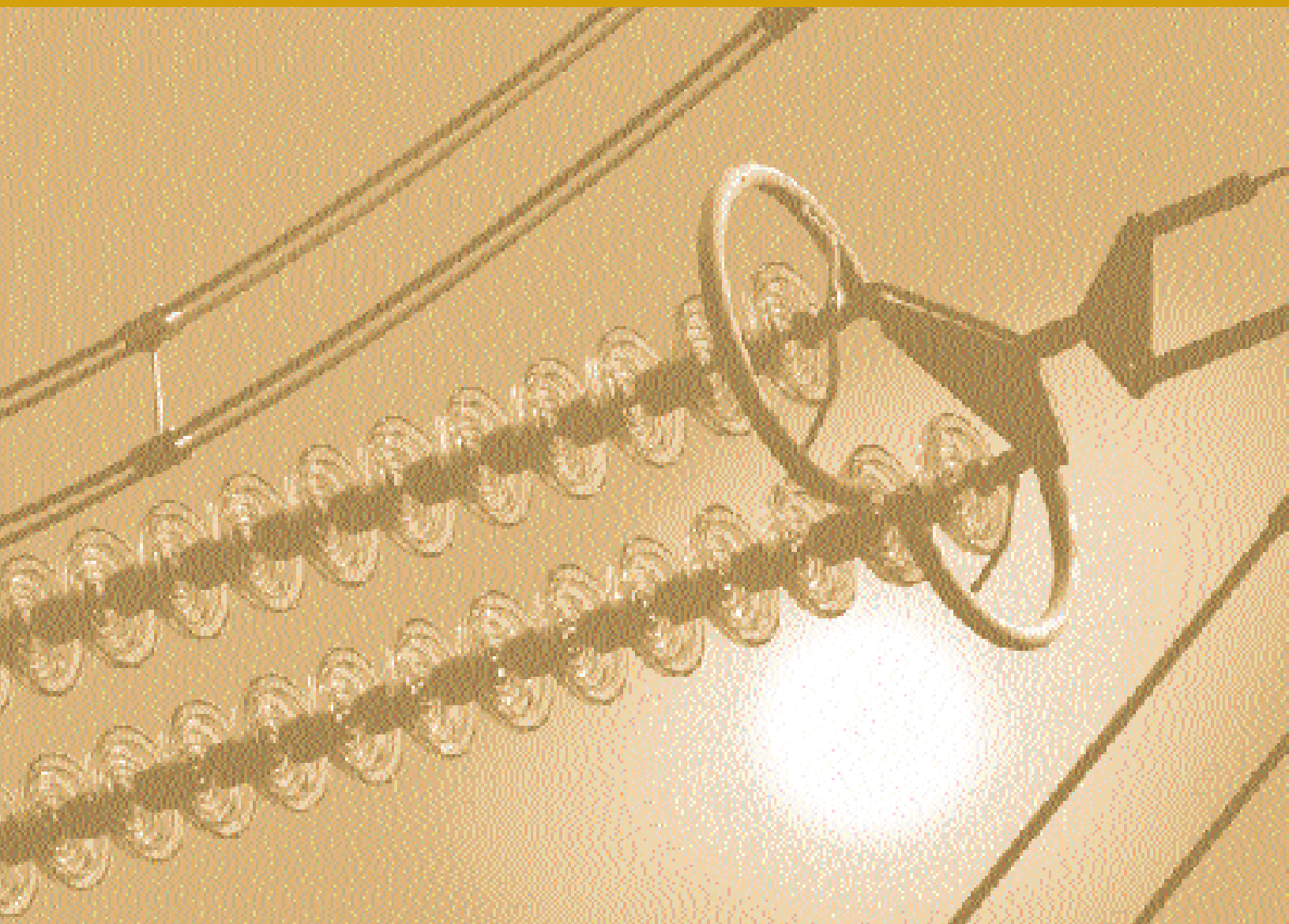
"To start with, we have to imagine the unknown and then help our companies prepare for it with a mixture of science, technology, psychology, logic, imagination, instinct, art and every other gift of the human mind we can marshall.

"It's also obvious, I think, that we can learn a great deal from one another. This discipline hasn't reached a point where it has a lot of rules set in stone. We are finding and creating answers all the time.

"We at PricewaterhouseCoopers welcome the opportunity to meet with you and share ideas about how we can all do this difficult job better."

For information about risk management and PricewaterhouseCoopers, contact:
Thom Barrett, Boston – (617) 478-5363
Barry Benjamin, Baltimore – (410) 783-7623
Rich Carson, San Francisco – (415) 498-7359

For questions regarding the Web cast available at http://webevents.broadcast.com/pwc/lyceumforum1201, contact Jennifer Murray at (617) 428-8165 or via e-mail at jennifer.a.murray@us.pwcglobal.com.



BOS.02-0700.01/02.LMT

www.pwcglobal.com

Your worlds  Our people