CENTER FOR INFORMATION SYSTEMS RESEARCH

Sloan School of Management

Massachusetts Institute of Technology

Cambridge Massachusetts

Developing a Common Language About IT Risk Management

George Westerman and Richard Hunter

June 2009

CISR WP No. 377 and MIT Sloan WP No. 4933-11

A version of this paper will be published as "Developing a Common Language About IT Risk," *IESE Insight*, Issue 1, Second Quarter 2009: 21–27.

☑ **Research Article:** a completed research article drawing on one or more CISR research projects that presents management frameworks, findings and recommendations.

☐ **Research Summary:** a summary of a research project with preliminary findings.

☐ **Research Briefings:** a collection of short executive summaries of key findings from research projects.

☐ **Case Study:** an in-depth description of a firm's approach to an IT management issue (intended for MBA and executive education).

☐ **Technical Research Report:** a traditional academically rigorous research paper with detailed methodology, analysis, findings and references.

CISR Working Paper No. 377

Title: **Developing a Common Language About IT Risk Management**

Author: **George Westerman and Richard Hunter**

Date: **June 2009**

Abstract: Although IT risks can have wide-ranging business consequences, few executives feel comfortable discussing IT risk management. It doesn't have to be this way. Executive-level tradeoffs around IT risk are managerial, not technical. The Four A Framework of Availability, Access, Accuracy, and Agility risks provides a common language that business and IT managers can use to manage IT risks without getting bogged down in technical complexity. Then you can build a risk management capability—by improving the IT foundation, installing a risk governance process, and creating a risk aware culture—that increases the returns from your IT risk management investments.

Keywords: IT risk, Non-IT executive viewpoint, IT governance, alignment, oversight, risk aware culture, architecture, business continuity, security, agility, regulatory compliance, privacy

9 Pages

Developing a Common Language About IT Risk Management

George Westerman, Research Scientist,
MIT Sloan Center for Information Systems Research
Richard Hunter, Vice President and Research Director, Gartner, Inc.

On Christmas Eve 2004, something unforeseen happened to ComAir, a subsidiary of Delta Airlines. The company's crew scheduling system failed. What happened next cost ComAir $20 million in revenue, untold losses in brand equity, a federal investigation, and the president of the company.

ComAir's scheduling system was antiquated in computer system terms. It had been scheduled for replacement five times by Christmas Eve 2004. Each time, the replacement had been rescheduled to make way for apparently more urgent work. The last time, in mid-2004, ComAir decided to delay replacement until early 2005. It was a costly decision.

December is always a busy month, and December 2004 was worse than usual. Bad weather forced ComAir to make more than 6,000 schedule changes between December 22 and 24 alone. Unbeknownst to anyone at ComAir, the scheduling system contained a critical field that could only count 32,767 changes in a month. At about 10 P.M. on Christmas Eve, a ComAir employee tried to enter the 32,768th change, and the system stopped dead. And, due to U.S. Federal Aviation Administration regulations, so did ComAir.

When the system failed, ComAir technicians realized to their dismay that the system could not simply be restarted. There was no backup system that could be pressed into immediate service. The only solution was to reload the entire system from scratch. They re-launched the system late on December 25, but by then ComAir had difficulty assembling crews and aircraft where they were needed. The airline didn't resume normal operations until December 29.

As the company struggled to recover from the disaster, about 200,000 stranded ComAir passengers helplessly roamed airport terminals throughout the United States. Television news followed the passengers through the terminals, broadcasting their distress to the American public throughout the Christmas holiday. Two weeks after the system failure, the U.S. Secretary of Transportation announced an investigation of the incident. A week later, ComAir's president resigned.

IT Risk is Business Risk

Up until ten years ago, information technology risk was not like this. Generally speaking, if a system failure or a security breach occurred, a mid-level IT manager dealt with it, and no senior executives (or the public) heard about it. Those days are gone forever, buried by laws such as California 1386, Sarbanes-Oxley and the European Union's Data Protection Directive, and by the public's massive adoption of personal computers and internet connections.

This working paper was prepared by George Westerman of the MIT Sloan Center for Information Systems Research and Richard Hunter of Gartner, Inc.

The ComAir incident created harm—to the public, to customers, to shareholders, and to senior company management. It excited the interest of regulators. Its total cost to ComAir, including loss of brand equity, was probably multiples of what the company spends on IT in a given year. It makes clear the emerging impact of IT risk in the 21st century, an era in which companies depend utterly on IT for everything from basic operations to executive decision making. That is why it is important for every executive to understand the kinds of risk IT creates for the organization.

To put it bluntly, IT risk is now business risk. Business executives—not just CIOs—ignore IT risk at their companies' and their own peril. And the converse is true as well: companies can use their IT risk management capabilities to improve the way they run their businesses and even to differentiate themselves from the competition.

Risk is Uncertainty, and Poorly Understood

Businesses respond more effectively to risks they understand, however unpredictable, than to the ones they don't. As an executive once said to us, "The risks I worry about most are the ones I don't know about." But of all risks to the enterprise, IT risks are often the least understood. Most managers do not know how to think about IT risk beyond the immediate impact on IT operations of viruses, security breaches, and continuity failures. They have not made the connection between failing machines and failing business operations. Or between taking shortcuts, or giving unclear guidance, and the inaccurate data and unnecessary corporate rigidity that result.

For many management teams, IT decisions are fraught with uncertainty. The likelihood and implications of system failure are uncertain. The implications of other IT risks, such as privacy lapses, data inaccuracies, project failures, or even corporate rigidity, are even more uncertain. All have complex causes and no perfect solutions. And they are all becoming more prominent every day.

ComAir's management deferred an upgrade to the crew scheduling system, and that decision had major consequences. Whether the decision was right or wrong is not the point per se; all managers make the best decisions they can every day based on incomplete information, and some are inevitably wrong. What matters is that the company's managers evidently did not understand the potential business consequences of failure in that mission-critical system, and so did not take steps to make such an incident manageable. To put it another way, the system failure was a symptom of failure to think through the risks and their response.

No one can make the right decision every time, but every company can build the capability to improve decision making around IT risk. Managers can start to ask questions that build more certainty around questions of risk. They can take action to reduce their largest risks. And they can create contingency plans to handle any incidents that arise.

Enterprises Need a Mature Approach

Most enterprises use an intuitive approach to IT risk management: they address high-profile risks that get media attention (such as viruses or power outages or wireless security), but

subsequently miss many risks that are lower-profile (such as inadequate internal controls or aging, brittle applications). In an era of deep business dependence on IT—and huge competitive, legal or regulatory impacts of IT incidents—this ad-hoc approach to risk management can no longer continue. Executives need a systematic and reliable way to make informed decisions about IT risk, and then ensure their risks are being managed.

That's why we started our IT risk research more than four years ago. We began by interviewing IT and non-IT executives in a dozen firms, followed by survey research with more than 130 firms around the world. We refined the messages and methods through teaching or speaking to more than 2,000 IT and non-IT executives and by in-depth discussions with more than 50 additional firms. The results, most recently published on our book, *IT Risk: Turning Business Threats Into Competitive Advantage* (HBS Press 2007), offer real-world frameworks and examples to help executives understand their IT risks and what to do about them.

The Four A Framework

There is no such thing as a risk-free (or risk-neutral) IT decision. Every IT risk has a business consequence. Small incidents often signal larger problems, and a series of small IT decisions can lead to large levels of business risk. Therefore, every IT oversight or investment discussion should consider the decision's impact on the firm's IT risks, not just the firm's strategic needs.

What is needed is a better way to make decisions—to clarify tradeoffs and then let both business and IT people do what they do best. We have found a way to do just that. If business and IT executives can focus on just four key IT risks, they can make better-informed decisions that lead to better IT (see Figure 1). The four risks are:

Availability: Keeping systems (and their business processes) running, and recovering from interruptions. ComAir is only one among many examples. Two times during August and November 2005, the Tokyo Stock Exchange (TSE) was able to trade only 90 minutes of its trading day due to a software glitch. Later, in January 2006, the TSE was forced to close early for several days when frantic trading in reaction to a news event exceeded the market's transaction-processing capabilities. Failure to manage uncertainties about transaction volumes and system reliability had huge impacts for ComAir and the TSE. Executives should know what their availability risks are for each major process, and should ensure there is a business continuity plan to respond in the event of failure.

Access: Ensuring appropriate access to data and systems, so that the right people have the access they need, the wrong people don't, and sensitive information is not misused. Many firms might worry about corporate espionage. But firms are often more exposed in terms of customers' or patients' personal privacy. Retailer TJX was sued for more than $300 million after a breach compromised 45 million credit card numbers. The June 2005 breach of 40 million credit card numbers at CardSystems, Inc. resulted in the demise and sale of the company. Executives should ensure their firms know who has access to what information, actively ensure people lose access when they leave the company and can trace exactly every access to sensitive information.

Accuracy: Providing correct, timely and complete information that meets the requirements of management, staff, customers, suppliers and regulators. Compliance with Sarbanes Oxley regulation in the United States is a clear source of accuracy risk. But so is the risk due to not having a clear view of the global supply chain or taking shortcuts in system development. The U.K. Inland Revenue paid out 2 billion pounds in erroneous tax credits in 2003–2004 after they installed a new system without adequate testing. Many firms are exposed to large and unknown levels of risk from inaccurate inventory records, "shadow" spreadsheets or the inability to get an accurate global view of key customers or product sales.

Agility: Being able to make necessary business changes with appropriate cost and speed. In the mid-'90s, electronics manufacturer Tektronix was forced to cancel the planned sale of a division because the division's systems could not be separated from the rest of the company's IT. It invested more than $50 million and three years to totally revamp its IT infrastructure and applications. While agility risk is not always as clear as that, most firms face some agility risk due to IT. Just ask yourself whether executives hedge on launch dates or hold off on big changes because they're not sure IT can deliver on time.

Discussing IT risks in terms of the four A's makes the uncertainty of IT risk more manageable. The four A's convert technical issues into business issues, and IT impacts into business impacts. It's often difficult (and uncomfortable) to make risky tradeoffs among abstruse technical complexities. But every effective executive can discuss costs and benefits in terms of the four A's. You can manage IT risk decisions the same way you manage all tradeoffs—by making informed choices among business alternatives.

The senior team of a rapidly growing medical transcription firm learned that they needed to replace their core system. The firm consisted of a small headquarters group managing a virtual workforce of 3,000 people working part-time from home. The company literally could not operate without its core system, but the existing system could not handle the growth expected in the next three years.

Two replacement options had strong merits at reasonable cost, but were designed very differently. One system provided bulletproof protection for availability and access risks at the cost of some agility. The other was much more agile, especially in terms of sourcing the workforce, but at the expense of increased risk in availability and access. And the senior team could not agree on which was best.

What seemed to be arguments over technology were really disagreements on what risks mattered most. The CIO favored the first option because it did everything possible to minimize the potential downside effects of availability and access risk. But the executive team eventually chose the second option, favoring agility over bulletproof availability or privacy protections. But the discussion helped them take an extra step. While they could not remove the potentially large downside of availability and access risks in the new system, they could cover themselves by investing extra money to make the new system better on these risks than any of their clients' internal systems. Focusing on key risks helped the executive team make

a better decision than they would have done by focusing on technology and costs alone. They protected the company's value proposition and strategic options, while defusing what could have been a heated argument.

Figure 1
The Four A Framework

Where Do We Start?

The first step in making risk-informed decisions is to get a handle on your firm's current IT risk profile. Start by discussing the executive-level questions with your colleagues and your CIO (see Table 1). It's likely that your senior team will have several different (and possibly conflicting) answers for each question. Or some questions may not have good answers yet. That's the point. By surfacing your preferences and opinions, you can come to consensus on the risks that matter most—what risks you need to resolve and which ones you can live with. You reduce uncertainty, both in the senior team and in your IT unit, and that goes a long way toward improving the way IT is managed. Without a clear answer on what risks are most important, business units make conflicting demands. Then the IT unit faces a near-impossible task of pleasing everybody. The inevitable result is complexity, risk and potential failure.

Next, operational managers can use the second set of questions in Table 1 to drill down on risks. How do the firm's business processes and skills, and IT systems and people, deliver on the desired risk profile? What should change to ensure risks are managed appropriately? And what risks remain, so that they can be tracked and managed in the future?

These questions help managers at all levels ensure their understanding of the meaning, potential consequences and relative importance of IT risks. They help bridge the gaps—between levels of the organization, and between IT and other parts of the business—so that everyone can make better decisions in a risk-informed way.

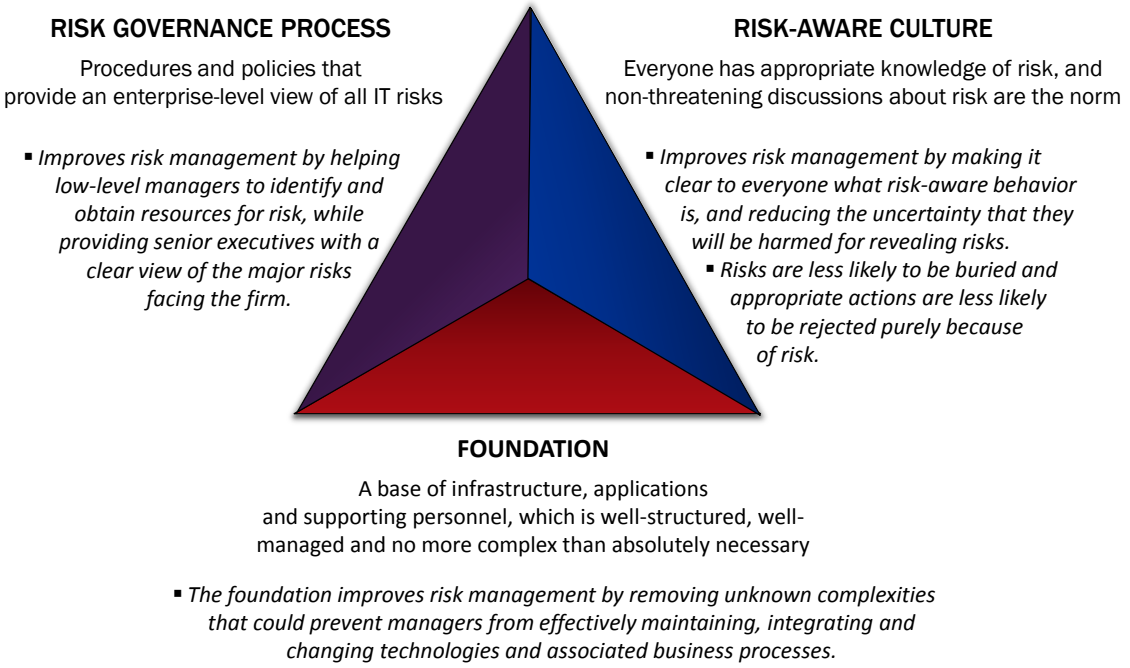
Table 1
Useful Questions for Discussing IT Risk

Executive-level Questions	Operational-level Questions
Availability	
▪ Which of our business processes are most dependent on IT? ▪ What consequences are likely if the systems are unavailable?	▪ What is the cost of a particular process being down for an hour? A day? ▪ What are our procedures to recover from interruption?
Access	
▪ What categories of information would be most damaging if released? For example, what is the likely impact of loss or theft of customer data? Product data? ▪ What categories of information are most important for our firm's daily success or failure?	▪ How do we control, protect and monitor access to these types of information? ▪ How can we ensure that the right people get access to this information as needed (and then lose access when done)?
Accuracy	
▪ Which processes and categories of information carry the highest consequences for inaccuracy (e.g., inventory information, financial information, etc.)? What would the firm lose if it could not maintain Sarbanes Oxley certification, for example? ▪ What constraints has inaccurate or incomplete information placed upon the organization? ▪ What could the firm do if it had better information in some area? For example, how much would the company save if it had better information on global customers?	▪ How can we improve the way that we gather or manage these types of information? ▪ How can we create or obtain valuable new types of information?
Agility	
▪ How well does IT currently deliver on new projects, and what does that mean for what the firm is able to do in the future? ▪ What major strategic changes (new product launches, new geographies, mergers and acquisitions, global cost-cutting, etc.) are foreseeable? ▪ What opportunity costs are entailed in missing a product launch (or other strategic move) by a month due to IT issues?	▪ How can managers in IT and business units improve project definition and delivery? ▪ What processes, skills and supporting systems are needed to support those changes? ▪ How should the IT foundation change to improve agility?

Three Disciplines to Improve Your Capability

Using the four A's to develop a common language about IT risk is a big step in the right direction. The next step is to implement three core disciplines of effective risk management (see Figure 2). These disciplines work together as a cohesive whole to improve the enterprise's risk profile and to keep it under control.

Figure 2
Three Core Disciplines of IT Risk Management



Fix the Foundation: The biggest driver of IT risk is complexity in the IT foundation. This complexity takes many shapes, including too many different types of hardware, too many applications integrated in unpredictable ways (if at all) and technology so old that few people understand the systems anymore. The complexity was not there at the start. It arose gradually over time, as IT people struggled to meet the needs of a diverse set of constituents. Every time IT people granted exceptions to standards, had to buy a new system that didn't fit with the firm's technologies or took a shortcut in response to an urgent business need, the IT foundation became more complex. Every merger or move to a new country increased complexity. And with complexity comes the risk of failure. Unknown vulnerabilities arise, recovery is difficult, and rapid change nearly impossible.

Our survey research shows that firms with a well-managed, simplified foundation have statistically significantly lower IT risk in *every* category of the four A's. A better structured foundation is easier to maintain, to control access and to recover in the event of failure. It is easier to develop a clear picture of information because each key piece of information is recorded correctly in just one place. And because IT assets and their links to business processes are better understood, business change is less difficult.

Fixing the foundation is rarely straightforward. Few firms can replace everything with a new IT platform like Tektronix did. Instead, every firm should first do the basics: ensuring that people who manage the foundation have the right skills and that processes have the right safeguards, controls, and monitoring. This includes ensuring you have a well-defined business continuity plan, so managers can react appropriately in the event that systems fail. Then, start to improve IT management processes and culture so that each major IT initiative moves the foundation in the direction of better structure, better management, and less complexity.

Implement Risk Governance Process: Identifying and prioritizing risks is fraught with uncertainty. A core dilemma of IT risk management is that the people most able to make enterprise level decisions about risk tradeoffs are those least capable of understanding or addressing risks throughout the enterprise. Top managers, who have the best enterprise-wide viewpoint to choose among risks, are farthest from the lower-level people who know what risks exist in the actual business processes. And vice versa.

A well-designed risk governance process manages the paradox. Strong policies, as well as clear methods to identify and assess risks, allow local managers to identify and assess risks in their areas (often with assistance from risk specialists), while providing higher-level executives an enterprise-level view of risks so they can make decisions. Beyond providing an enterprise view of risks, the risk process also creates a sense of order and control. It reduces uncertainty and instills confidence, inside and outside the enterprise, that IT risk is being managed appropriately. Furthermore, it can help executives make other IT decisions more effectively because they have a view of risk as well as potential return.

Build a Risk-aware Culture: Executives' most important role in IT risk management is to build a culture of risk awareness. Employees at all levels must understand how their decisions and activities either increase or decrease risk. They must understand what danger looks like (such as a server reaching capacity or a contractor behaving irresponsibly) and how to prevent it or report it to the right people. They need to understand what policies and rules exist, and why they are important.

But risk awareness goes beyond that. If the most dangerous risks are the ones that the organization has never anticipated, then the most important thing executives can do is encourage employees at all levels to speak openly about risks. This is the meaning of a risk-aware culture: it is a culture in which employees feel free to discuss risks and ask for help. If people are not comfortable discussing risk, one of two bad things happens. They may decide to hide their risks, hoping they won't blow up later. Or they may become so risk averse that they become rigid gatekeepers, creating unknown risks as people choose to work around them rather than with them.

The most important thing managers can do to create such a culture is to practice two responses. First, when an employee comes to the manager and says, "I have a problem," the manager should say, "Tell me about it." Then, when the employee has finished describing the risky situation, the manager should respond, "You will get help," and make sure it happens.

The result is a culture that reduces uncertainty about IT risk by making it very plain what risk-aware behavior should be. When everyone knows what to expect from themselves and their peers, they can work together to manage risks and achieve great things.

Building the three disciplines—foundation, process, and culture—does more than help the enterprise manage IT risks better. It also gives executives *confidence*. In our study, firms that were more confident in their IT risk management capabilities reported more control over all four IT risks, they were significantly less likely to say they were unaware of important IT risks, and they enjoyed significantly better relationships between IT and business executives—all while spending only fractionally more than other firms on IT risk management.

Risk Management is More Than Avoiding Risk

No enterprise can eliminate IT risk, and capable risk managers know it. Firms that succeed in business do not eliminate risk; they manage it. Firms with solid IT risk management capability also know something else. By making risk management part of everything they do with IT, they gain benefits beyond reducing risk. Discussing risk as well as return helps ensure systems and projects deliver what they are supposed to deliver. It balances short-term need with longer-term risk, helping convince executives and staff to follow good IT management practices, even when they would prefer not to. And, as risk management becomes instilled into the culture, fewer and fewer people will need to be convinced to follow good management practices, because good practices will become just another part of doing business.

Firms that consider IT risk management as nothing more than a cost of doing business—a way to avoid bad things—get what they expect. They invest money and avoid bad incidents. But as our research shows, firms that see IT risk management as a key capability gain much more. Beyond avoiding bad incidents, IT risk management helps them identify and justify valuable improvements such as removing redundancy, integrating information, and making business processes smoother. And, over time, their firms become more agile; they can successfully capture valuable business opportunities that their competitors would consider too risky to pursue.

Tektronix found that its newly designed IT foundation did more than enable the firm to sell a division. It also improved business performance by increasing inventory turnover, speeding credit processing and smoothing integration of acquisitions. Financial services provider PFPC implemented risk management to avoid incidents and then used it as a key tool to improve IT management processes and transform aging systems. Soon, salespeople started inviting the CIO on sales calls to explain why it was safer to do business with PFPC than with their competitors. Any firm can convert IT risk management from a cost to a source of advantage as long as executives are willing to give it their sustained attention. IT executives can do much of the work to implement IT risk management capabilities. But true advantage comes when all executives use those risk management capabilities to manage IT—and the business processes that depend on it—better than they ever have before.

MIT SLOAN CISR MISSION

MIT CISR was founded in 1974 and has a strong track record of practice-based research on the management of information technology. MIT CISR's mission is to perform practical empirical research on how firms generate business value from IT. MIT CISR disseminates this research via electronic research briefings, working papers, research workshops and executive education. Our research portfolio includes but is not limited to the following topics:

- IT Governance
- Enterprise Architecture
- IT-Related Risk Management
- IT Portfolios and IT Savvy
- Operating Model
- IT Management Oversight
- Business Models
- IT-Enabled Change
- IT Innovation
- Business Agility
- The IT Engagement Models

In July of 2008, Jeanne W. Ross succeeded Peter Weill as the director of CISR. Peter Weill became chairman of CISR, with a focus on globalizing MIT CISR research and delivery. Drs. George Westerman, Stephanie L. Woerner, and Anne Quaadgras are full time CISR research scientists. MIT CISR is co-located with MIT Sloan's Center for Digital Business and Center for Collective Intelligence to facilitate collaboration between faculty and researchers.

MIT CISR is funded by Research Patrons and Sponsors and we gratefully acknowledge the support and contributions of its current Research Patrons and Sponsors.

CONTACT INFORMATION

Center for Information Systems Research
MIT Sloan School of Management
5 Cambridge Center, NE25, 7th Floor
Cambridge, MA 02142
Telephone: 617-253-2348
Facsimile: 617-253-4424
Email: cisr@mit.edu
http://mitsloan.mit.edu/cisr

Mission and Contact Information as of August 1, 2009.

CISR RESEARCH PATRONS

The Boston Consulting Group, Inc.
BT Group
Diamond Management & Technology Consultants
Gartner
IBM Corp.
Microsoft Corporation
Tata Consultancy Services Limited

CISR SPONSORS

Aetna, Inc.
Allstate Insurance Company
ANZ Banking Group (Australia)
Banco Bradesco S.A. (Brazil)
Banco Itaú S.A. (Brazil)
Bank of America
Biogen Idec
BP
Campbell Soup Company
Canadian Imperial Bank of Commerce
CareFirst BlueCross BlueShield
Caterpillar, Inc.
Celanese
Chevron Corporation
CHRISTUS Health
Chubb & Son
Commonwealth Bank of Australia
Credit Suisse (Switzerland)
CVS Pharmacy, Inc.
Det Norske Veritas (Norway)
DHL Global Management GmbH (Germany)
Direct Energy
Embraer – Empresa Brasileira de Aeronautica S.A. (Brazil)
EMC Corporation
ExxonMobil Global Services Co.
Fidelity Investments
Grupo Santander Brasil
Guardian Life Insurance Company of America
Hartford Life, Inc.
HBOS Australia
Intel Corporation
International Finance Corp.
Johnson & Johnson
Liberty Mutual Group
Marathon Oil Corp.
MetLife
Mohegan Sun
NASA
Nomura Research Institute, Ltd.
Parsons Brinckerhoff
PepsiAmericas, Inc.
PepsiCo International
Pfizer, Inc.
PNC Global Investment Servicing
Procter & Gamble Co.
Raytheon Company
Renault (France)
Standard & Poor's
State Street Corporation
Sunoco, Inc.
TD Bank
Time Warner Cable
Trinity Health
Unibanco S.A. (Brazil)
VF Corporation
Wal-Mart, Inc.
World Bank