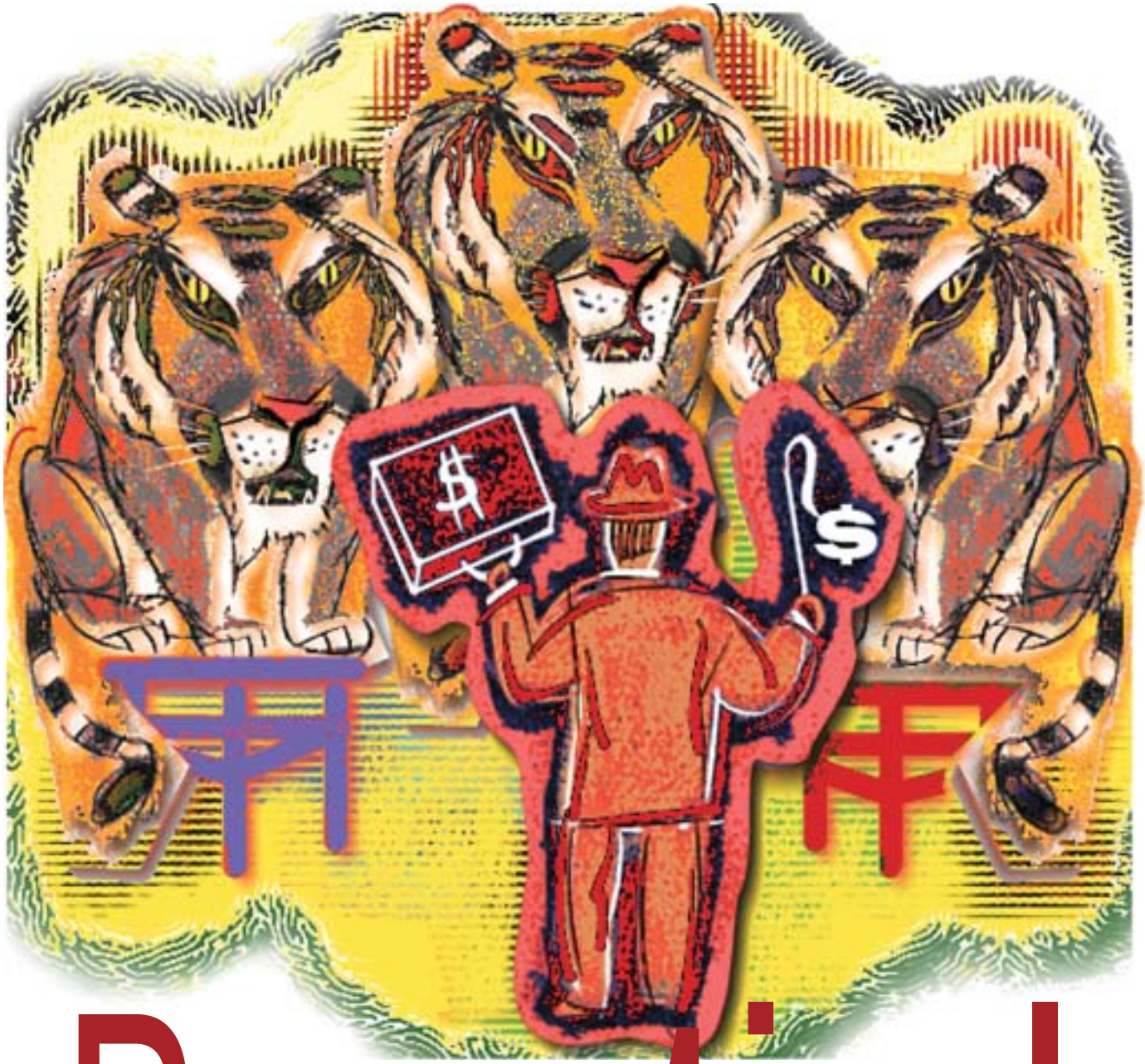
Managing Risk

WITH 9/11 and Enron still engraved in our memories and a slew of new regulations to follow, companies and boards are taking a more proactive stance in developing and implementing systems to manage risk throughout their organizations. Some best-in-class firms like Pfizer Inc. have created complete departments focused on corporate governance and enterprise risk management (ERM). Pfizer's was up and running long before 9/11. But scores of other companies are only now awakening to the need to develop more sophisticated protocols and systems to manage risk.

"The bottom line is that (9/11) brought the awareness level to a much higher degree of focus and importance in organizations," says Michael J. Chagares, a business risk consultant at Marsh USA Inc., a risk and insurance services firm. During the bull market, he adds, the risks in companies were often masked behind a strong financial performance. Consequently, many firms tended to be less proactive and more reactive regarding risk matters.

But now companies have done a somersault and are managing risk of all types more aggressively. Ted Senko, partner in charge of management assurance services at KPMG LLP, which advises companies on risk management practices, agrees the landscape has changed. "Stakeholders are more attuned than ever to corporate risk," he notes. "Some of the sensitivity of 9/11 has dulled, but I believe the bar has been raised in terms of managing risk due to the corporate scandals."

ILLUSTRATION: SUSAN LEVAN/ARTVILLE



Proactively

By Bruce W. Fraser

Today, experts agree there is far less tolerance by stakeholders for not being prepared for disaster. "The longer you move away from Sept. 11, the reaction of stakeholders becomes far more harsh," Chagares says. "Now you have a legislative push by the Securities & Exchange Commission and others, the Sarbanes-Oxley Act, and a lot of other reasons why companies are starting to re-evaluate all this."

The upshot is that "boards, stakeholders, executive management are all looking for more broad and anticipatory ways to manage risk in order to achieve their strategies, objectives, and performance goals," Chagares explains. "This process helps companies focus on the cause of risk versus treating only the symptoms, i.e., the effects. You're focusing on curing the disease, not just tangentially dealing with the symptoms."

How is ERM being viewed and used in organizations post 9/11? How have attitudes changed? How does a company assess its risk across the enterprise? What steps are involved in implementing a risk management program?

To give readers some insights, *Strategic Finance* looked at three companies proactively managing risk today. Two, J.P. Morgan Chase & Co. and Royal Bank of Canada, have mature systems in place. The third, J.A. Jones Inc., is just beginning the journey.

JPMORGAN CHASE

In the context of running a company, operational risk management has been defined as managing the risk of loss resulting from inadequate or failed processes or systems, human factors, or external events.

JPMorgan Chase has designed and implemented a broad framework to identify and control operational risk across all levels of its global operation. "Our goal has been to improve both our understanding of the causes of operational risk and the management of those risks and thereby improve overall financial performance," says Barry Macklin, senior vice president of JPMorgan Chase Treasury and Securities Services.

"We need to have an operational risk model that has authority and accountability," he continues. "We want to provide risk tools that promote internal and industry leading practices. We also want to be able to implement a capital framework incorporating incentives to encourage investments in the control environment."

Other goals include "being able to integrate the operational risk framework with other business activities, being able to monitor and report the types of operational risk to senior management, and benchmark results against performance."

Part of the effort has been "to share 'best practices' in operational risk management across all our business units so we can benefit from the shared knowledge and learn from our capabilities, efforts, and mistakes," adds Joe Sabatini, managing director and head of corporate operational risk for the firm.

A crucial necessity for such a program to exist, whether at JPMorgan Chase or any other company, is a culture of openness. Notes Macklin: "You must have a partnership between your business managers, who own their control environment, and audit, finance, and risk management professionals. You need a commitment from all these parties to work together."

Broadly speaking, an operational risk event can occur in any one of at least five different categories, according to JPMorgan Chase:

1. Clients, products, and business practices. Risks could stem from suitability issues or from a breach of fiduciary duties. Both are red flags, especially at financial institutions;

2. Fraud, theft, and unauthorized activity, e.g., unauthorized trading or money laundering;

Warning!

Here's a list of potential warning signs that signal your company may need enhanced risk management:

- ! A disaster caused by natural or human means.
- ! Changes in company's business model.
- ! A major acquisition or new business venture that results in a flawed integration process.
- ! Earnings surprises/earnings restatements.
- ! Regulatory or legal problems.
- ! Frequent leadership changes.
- ! Major operational breakdown.
- ! Bankruptcy of key supplier or vendor.
- ! Major product recall.
- ! Reading about any of the above on the front page of your local newspaper.

3. Execution and processing errors, e.g., a system failure or a trade entry error;

4. Employment practices and workplace safety, such as wrongful dismissal, harassment, or workers' compensation issues; and

5. Physical asset and infrastructure damage, for instance, a natural disaster or a human instigated act of damage.

JPMorgan Chase employs a number of tools to control operational risk. One is a Web-based self-assessment process and application tool, known as "Horizon," which is used to assess and manage enterprise-wide risks. It enhances the quality of the firm's control self-assessment program, improves efficiency, and strengthens risk management skills. "Horizon's Web-based technology helps us share risk expertise and best practices across our lines of business and is essential to identifying and controlling risk in our global operations," Macklin says.

An integral part of the firm's operational risk program is a governance structure that promotes transparency and accountability of each business and support unit. In addition, the bank uses key performance indicators to identify developing control issues and earlier this year implemented an automated risk-event database that tracks operational losses. Currently under development is a model for assigning operational risk control and integrated risk management architecture.

"Some of the tools are more advanced than others," Sabatini says. "It's a work in progress, and while each initiative on its own is worthwhile and valuable, it's the ability to integrate these and understand the relationship components that will create an environment of continuous improvement."

ROYAL BANK OF CANADA

In the Internet age, privacy has become a central issue. While many companies address privacy because of regulatory demands, and others give it cursory attention, some firms are turning this risk into opportunity.

The Royal Bank of Canada, based in Toronto, has tackled privacy risk management head-on. Its privacy policy is centered on retaining and growing customers' trust, and it's an integral part of the bank's business strategy and everyday practices.

"The core is that customer information use is absolutely key to our business strategy, and it's a key expectation of our customers that we leverage the information to provide them with value while also protecting and keeping it private," says Peter Cullen, corporate privacy officer of RBC Financial Group (the brand name of Royal Bank of Canada).

Royal Bank of Canada is that country's largest financial institution measured by market value and assets, and it has a large U.S. presence. The bank has had a privacy policy in place since the mid-1980s. Several years ago the bank began to think about privacy as an emerging business issue and one where it felt it could achieve competitive differentiation. The result was an aggressive strategy

Marsh USA's Prescription

Here's some advice from Marsh USA for a successful corporate risk management program:

LEADERSHIP AND SPONSORSHIP

You need executive-level sponsorship and leadership for the program to be successful.

CULTURAL AND BEHAVIORAL CHANGE

It requires cultural and behavioral change, meaning your company can no longer do things and manage things status quo.

OWNERSHIP AND COMMITMENT

The operating management and business owners have to take ownership and be committed to the program. It's a long-term rather than short-term way of managing their business.

DISCIPLINED AND OPEN APPROACH

There must be a formal structure and framework in place. The approach has to be transparent. When risks are identified and prioritized, information has to be shared across the board.

TIME AND RESOURCE DEDICATION

Creating a risk management system doesn't happen overnight. To develop, design, and implement such a program can take anywhere from six months to three years, depending on the size and complexity of the company.

CONTINUOUS PROCESS IMPROVEMENT AND FEEDBACK

You don't have to wait until you have the perfect process in place. Your system will become better over time.

to manage both the risks and opportunities of privacy management. This meant aspiring to a higher level beyond merely meeting regulatory requirements.

"This is a customer trust issue that has to be managed as such, and it's also an area of competitive differentiation," Cullen explains. "We looked at it through a lens of how we could do things differently as it's really tied to our business strategy as opposed to merely meeting a regulatory hurdle. The risk is not managing to a regulatory authority; the risk and opportunity is managing to a customer expectation."

Based on customer research, "83% of our customers would leave if they felt their information was being listed inappropriately or was not being well protected," Cullen adds.

"The issues for us are how to earn customer respect around the use and protection of their information. If you're going to take a proactive stance with your customer and communicate how well you respect that core tenet, you need to ensure you have policies and practices that can back that up," he advises.

The multinational organization manages risk in an integrated but matrix manner, Cullen explains. Key business leaders in each of the institution's lines of business in vital geographic areas are under a mandate to champion and be accountable for privacy management processes in their area. "Everything we do—every process we develop—has the customer balance at its root," he says.

One area the bank is managing proactively is its websites. Sustaining customer trust online is a critical area at the bank. RBC Financial Group maintains more than 25 websites and over 50,000 Web pages—all potentially capable of collecting personal data. These sites are managed by independent departments, business units, and functional units.

Privacy at the bank is also a strong driver of its brand identity. Privacy accounts for an estimated 14% of overall brand value and 7% of overall shareholder value, indicating that privacy is more important to the brand than to driving business. This in itself supports the bank's view that customers associate the perception of the bank strongly with how well customer privacy is managed.

J.A. JONES INC.

Likewise, J.A. Jones, a $3 billion global diversified services company, is developing a risk management tool that can be used at all levels throughout its organization.

"We're actually drilling it down so our line management can use it as a tool to manage risk," says Eric J. Gerner, vice president of corporate risk strategies. "In many ERM processes, you have a facilitator who helps take a current snapshot of risks and moves on. Instead, we're trying to create an ongoing management, measurement, and monitoring tool to be used across all levels of the company."

J.A. Jones, based in Charlotte, N.C., began developing its risk management system in October 2001 in order to take a more structured and proactive means to managing key risks.

At the outset, CEO Al Neffgen had a number of goals, according to Gerner. One was to create a centralized risk management process that could be coordinated with technical experts in all areas of the company. Another goal was to be able to aggregate and quantify key risks for business decisions, including capital allocation. The company also wanted to find the best way to monitor the risk/reward relationships. In short, it wanted to create a simple process and integrate it with day-to-day practices.

"This doesn't change who's responsible for managing the risks, and it's not a replacement for good judgment," Gerner notes. "Our aim was to provide a good decision-making process for good judgment. We want people identifying, planning, and communicating key risks as early as possible. The framework creates that ability."

The next step was to come up with a list of all possible risks across all levels of the company. "When we sat down to figure out what the key risks were, we came up with about 300, then narrowed them down to about 75," Gerner says. The 75 make up J.A. Jones's risk universe, or risk mapping structure, which essentially attempts to address all the key risks across all areas of the firm.

"It was basically creating a means for structured brainstorming of key risks to get everybody thinking of the broad areas of risk and then structuring the process so we can aggregate, measure, manage, and monitor it in a structured way."

Gerner says J.A. Jones is trying to leverage its risk management program so it can be used to its best advantage. "When we view risk, we look not only at the negative things that can happen but also at the opportunities to leverage risk to our benefit," he explains. "We recognize risk is a normal part of our business. There is no business that has no risk. The trick is to effectively manage risk and create strategic opportunities from it. We're not done with this yet. We're about halfway through our journey." ■

Bruce W. Fraser is a freelance writer based in New York City. You can reach him at frasernyc@aol.com.