

MMC

MARSH MERCER KROLL
GUY CARPENTER OLIVER WYMAN

Viewpoint

Issue 2 2009

Our Leading Thinking on Today's Critical Issues and Risks



The Hard Part: Strategy Execution

**Bridging the Gap Between
Vision and Action**



Combating Pay Equity Risk in a Recharged Climate

**Pay Discrimination Suits in a New
Era of Federal Scrutiny**



Confronting Fraud in a Downturn

Scams and Evolving Risks



Enterprise Risk Management Did Not Fail in 2008

Look Deeper for the Underlying Causes



Risk Management and Economic Change

**A Catalyst for Re-evaluating Business
Preparedness, Mitigation and Response**

The Businesses of Marsh & McLennan Companies

Risk and Insurance Services Marsh
Guy Carpenter & Company

Risk Consulting and Technology Kroll

Consulting Mercer
Oliver Wyman



MARSH MERCER KROLL
GUY CARPENTER OLIVER WYMAN



viewpoint

Issue 2 2009

Our Leading Thinking on Today's Critical Issues and Risks

Editor Patricia Gatto-Puglia

Editorial Offices Marsh & McLennan Companies, Inc.
1166 Avenue of the Americas
New York, N.Y. 10036
Telephone: 212 345 5485

Illustration Dave Cutler: cover, p.iv
Kamalova: cover, p.12
Kamalova: cover, p.22
Michael Aveto: cover, p.32
Rob Day: cover, p.40

Design and Production Rachelle Nidra Somma, New York, N.Y.

©2009 by Marsh & McLennan Companies, Inc.

This and previous issues of *Viewpoint*
are available at www.mmc.com/knowledgecenter

Our Leading Thinking on Today's Critical Issues and Risks

Viewpoint

Issue 2 2009

Table of Contents

- 1** **The Hard Part: Strategy Execution**
Bridging the Gap Between Vision and Action

■ By Mark Nadler



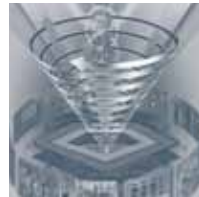
- 13** **Combating Pay Equity Risk in a**
Recharged Climate
Pay Discrimination Suits in a New Era
of Federal Scrutiny

■ By Michael Burniston and Brian Levine



- 23** **Confronting Fraud in a Downturn**
Scams and Evolving Risks

■ By Richard Abbey, Alan E. Brill and Brian G. Lapidus



- 33** **Enterprise Risk Management**
Did Not Fail in 2008
Look Deeper for the Underlying Causes

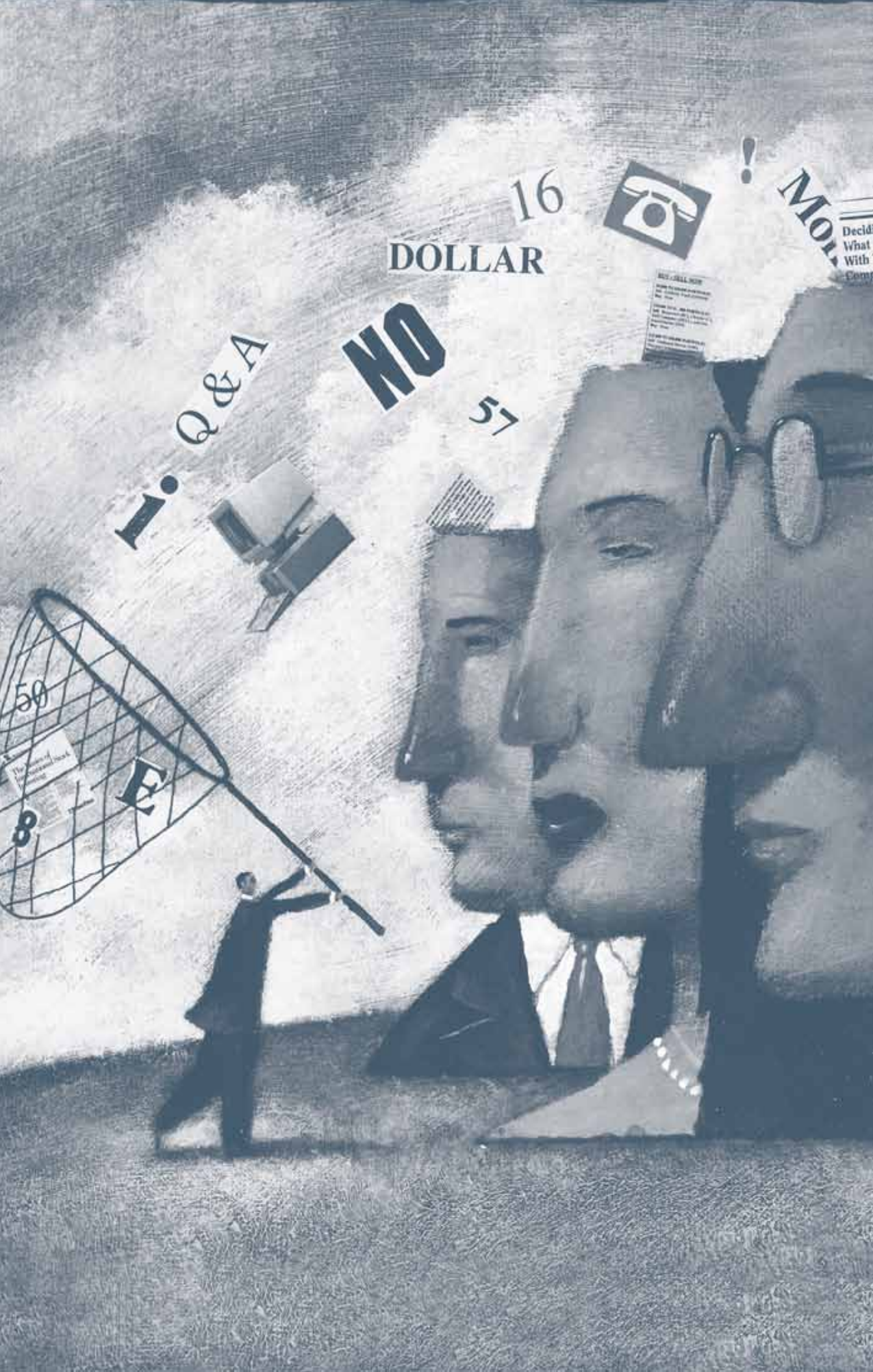
■ By Donald Mango



- 41** **Risk Management and Economic Change**
A Catalyst for Re-evaluating Business
Preparedness, Mitigation and Response

■ By Gary S. Lynch





DOLLAR

16



!

MOI

Decid
Wha
With
Comp

Q&A

NO

57



59

8

E

The number of...
back...

The Hard Part: Strategy Execution

Bridging the Gap Between Vision and Action

We seem to be easing our way into the third phase of the economic crisis. First came the initial shock to the global financial system, fueling an economic collapse. Then came the realization that this was no blip, but rather the beginning of a long, deep, painful downturn. That launched a cascade of downsizing announcements – factories shuttered, stores closed, jobs wiped out, pay and benefits slashed.

by Mark Nadler

However, that grim outlook has nudged many companies from the purely defensive tactic of downsizing to a more offensive posture, as they have sought new strategies to come to grips with changes that are transforming the marketplace with stunning speed and effect. The third phase has been characterized by the emergence of new competitive strategies. The playbooks vary enormously; some businesses and industries – print media and home construction, for instance – have been more seriously affected, with many seeking strategies for survival. For others, the underlying business has not vanished – health care, for instance – so the strategic challenge has been how best to weather the storm in order to emerge in good shape and, hopefully, an improved competitive position.

Whatever the case, and in any economic scenario, leaders must find ways for their companies to simultaneously shrink and grow. To do that, they must unfreeze any organizational paralysis that might have set in earlier this year by articulating a clear vision of where they want the organization to go, and then successfully executing the strategies to get things moving.



And there's the rub. Even in the best of times, few companies are consistently adept at implementing strategies. Consider a few dismal numbers:

- A 2004 survey of 276 senior operating executives by *The Economist* found that 57% of the companies had been unsuccessful in executing on strategic initiatives over the previous three years.
- In a 2006 survey of more than 1,500 executives by the American Management Association and the Human Resource Institute, only 3% of respondents rated their companies as very successful at executing corporate strategies, while 62% described their organizations as mediocre or worse.

Strategy execution tends to be a hit-or-miss proposition. Based on our experience, there are some common pitfalls that deserve attention. This isn't intended as an exhaustive guide to strategy implementation, but rather a checklist of potential stumbling blocks that senior leaders should consider before launching a strategy initiative. Ignore or mishandle any one of them and they could slow the initiative down, trip it up, or send the entire cart sliding into the ditch. By the same token, making sure all these bases are covered will go a long way toward increasing the odds of success.

1. Good strategy, bad process

The basic principle is simple: The people senior leaders rely on to implement the strategy should have a say in developing it. The most important thing one can do to improve the quality of execution is to ensure that the managers who will have to fire up the troops and personally fight the daily battles required to implement a grand vision have been afforded opportunities for appropriate participation.

There are many credible excuses for not broadening the process. It's messy, time-consuming, and often results in uncomfortable, even volatile, confrontations. It requires discussing some highly sensitive issues involving priorities, resource allocations, major shifts in markets or offerings, or new structural arrangements that would be easier to announce than debate. But there's no surer way to derail a strategy than for senior leaders to lock themselves away—or hand it off to consultants—and then dump it on managers with the instructions, “Go make it work.” They won't.

More often than not, resistance sets in and can take a passive-aggressive form. At a nationally respected health organization, the CEO closeted himself with consultants and brought forth a brand new strategy, which made his direct reports feel disrespected and disenfranchised. So, when asked about how the strategy was being implemented, they responded almost universally: “It's a wonderful vision, but I have absolutely no idea how we're supposed to make it happen.” Until the CEO retraced his steps, brought his team on board, and let them dissect, rebuild, and own the strategy, almost nothing happened.



Participation, and the buy-in that comes with it, are essential to successful implementation. Even if executives have already started down the path of strategic development, they can still involve the right people before the strategy is set in stone.

2. Strong strategy, weak alignment

Not everyone in management can be personally involved in developing the strategy. But everyone in management should understand it, accept it, and be committed to its success. That's not always the case. We constantly hear people in senior management positions say, "I know what the CEO says the strategy is, but I have no idea what that really means."

Not long ago, we were asked to work with a multibillion-dollar manufacturing company that had recently been formed by the merger of two moderately successful companies. Things got off to a reasonably good start, but as the first year came to a close, financial results unexpectedly plummeted. At a daylong session involving the top 40 or so executives, all the possible operational breakdowns were scrutinized. Picking up on undercurrents in the room, we raised the issue of strategic alignment and were firmly assured by the CEO that everyone was "on board" and strategy was not an issue. Just to be sure, we had everyone write a two-sentence description of the company's strategy; we then read seven of them at random and ended with what the CEO had written. None of the eight statements were the same and some were in direct conflict, with the top priority variously described as profitability, market share, and reputation for quality and innovation. The CEO reluctantly acknowledged there was an enormous alignment problem across management—and immediately made that the first priority coming out of the session.

Understanding the substance of the strategy is just the first step toward alignment. Once managers understand the strategy and its implications, the next goal is acceptance. And for truly effective execution, you need managers to go beyond passive acceptance to active commitment. As a CEO prepares for implementation, he or she should be absolutely certain where key managers are on the scale of understanding, acceptance, and commitment, and should move them up the scale before getting too far down the road.

3. Right strategy, wrong team

New strategies create new requirements for leaders, and the more radical the shift in strategy, the greater the need for senior people with fresh perspectives, skills, experiences, and leadership styles. The unfortunate paradox is that the management team that was responsible for past success could actually constitute the greatest obstacle to future survival.

In his book *Only the Paranoid Survive*, retired Intel CEO Andrew Grove recalls one of the more poignant moments as the company began its transformation from manufacturing semiconductors to producing microprocessors, an enormous shift in technologies and business models. At an executive staff meeting, Grove looked around the room and wondered how many of the people there, all of whom had played key roles in Intel's success, would survive the transition. The eventual answer: about half.

Any genuine shift in strategy implies a change in emphasis; it might involve different customers or markets, new technologies or business processes, unfamiliar leadership styles or management techniques. This requires that leaders learn new skills and master new approaches – a big

challenge in itself. Even more problematic, a new strategy undermines the organization's political profile in very tangible ways. It alters priorities, resource allocations, and reporting relationships. It threatens the power, status, scope of responsibility, and business philosophies of important and influential people. Some will be incapable of learning new skills, whereas others will be unwilling to accept a revised role, much less a different approach to doing business. Whether they are unwilling or unable, some members of the senior team simply need to move on; the longer they stay in place, the more difficult it will be to implement the new strategy.

4. Leaders without followers

Up to this point, we've been focusing primarily on the senior team and other top managers, since that's where strategy implementation has to start. But it can't end there, because execution also fails when a discernible gap opens up between the top echelon and the rest of the organization. There's a tendency to attribute that gap to "poor communication," and sometimes, that's actually the answer.



But often the problem goes beyond communication – it's less about sharing information than about shared interests. A few years ago, we did some work with a global consumer products company that was preparing to launch a strategic initiative they were going to call "Simplification." To the executives who planned the initiative, the ultimate goal was to eliminate layers of management, increase accountability, accelerate decision-making – and, in the process, cut several thousand jobs. The rest of the organization, however, having experienced successive waves of job reductions, demonstrated a remarkable degree of skepticism, if not outright disbelief. From their

perspective, this was all about slashing the payroll, and everything else was window dressing. Resistance was strong, implementation was difficult, and after a while even senior leaders did their best to distance themselves from the effort.

The reverse is also true. At Quest Diagnostics, the nation's largest provider of medical testing, a strategic pillar of the company's turnaround in the mid-1990s was an unprecedented emphasis on providing the industry's "gold standard" of quality services. That was a serious departure from the previous strategic priority, which involved billing hospitals, doctors, and patients for as many tests as possible and resulted in millions of dollars in government fines related to billings for tests that had never been asked for. The "quality" strategy resonated with employees – from highly trained pathologists to lab technicians overseeing routine, automated tests – in ways that far surpassed management's expectations. Why? Because the strategy was a perfect match with the values of the vast majority of employees, who had chosen this kind of work specifically because they wanted to feel part of a noble social endeavor. The focus on quality engendered a sense of pride and a connection to the organization that was clearly reflected in effective recruitment, retention, job performance, and ultimately, in the company's impressive financial success.



5. Conflicting strategy and tactics

There's another disconnect that can easily derail strategy implementation: a perceived conflict between the strategic vision and the supporting tactics. The former tends to be lofty, the latter tends to be brutally pragmatic, and the discrepancy calls into question top management's commitment to its stated values.

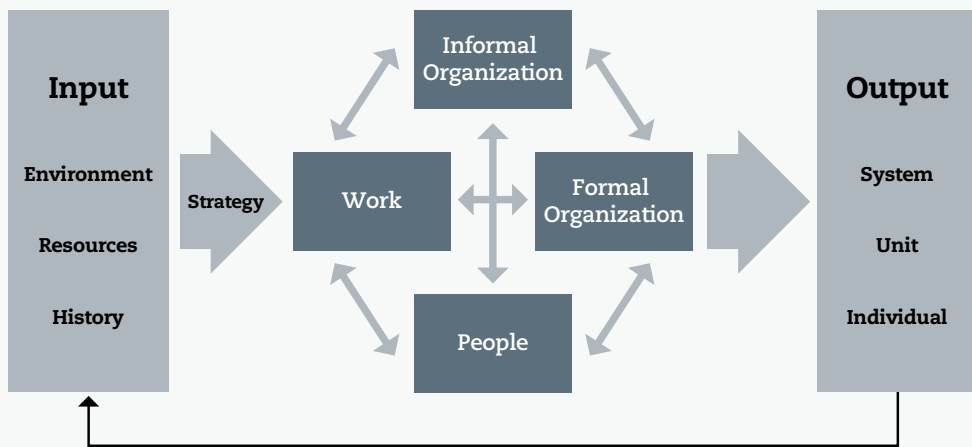
Consider a global telecommunications company that, in the wake of a merger, adopted and communicated a strategy based on product innovation and strategic alliances. Most people in the company felt good about the change; it appealed to their sense of professionalism. But it soon became clear that it would take time for the new strategy to generate substantial revenues; for the time being, most of the revenue would continue to flow from the original business model, which relied largely on locking unsuspecting customers into long-term subscriptions they really didn't want. The difference between the articulated vision and the actual tactics nearly brought the company to its knees; senior leaders lost credibility and were replaced, top performers felt betrayed and went elsewhere, revenue fell far short of plan, and nearly a year of valuable time was lost as the business was patched back together.

6. Changing the pieces, not the puzzle

Until now, we've been talking about specific pieces of the strategy puzzle. But from an organizational perspective, the only sensible way to think about strategy execution is to step back and keep your eye on the entire puzzle.

For years, we've used a fairly simple and practical way of describing that organizational puzzle. Every organization, no matter how simple or complex, consists of four basic components: the activities that constitute the organization's core work; the people who manage and perform that work; the formal structures that determine where work gets done and who reports to whom; and the set of values, beliefs and behavioral norms – culture, if you will – that guide people's performance and interactions.

Exhibit 1 The congruence model of an organization



Source: Oliver Wyman Delta

The tighter the fit, or "congruence", among all four components, the better the performance (Exhibit 1). Make a significant change in any one of the four, and it's like trying to jam the wrong piece into a jigsaw puzzle – the adjoining pieces get shoved out of place. Introduce a new strategy, and odds are you'll have to come up with an entirely new organization.

Think about the telecommunications company mentioned earlier. The new strategy – enticing customers to make rational and informed buying decisions rather than roping them into long-term commitments – set up a visible clash between the newly espoused values and the actual business practices. Beyond that, the company lacked the talent it needed to implement the new strategy – product

development was seriously understaffed in comparison with sales. And even if they'd had the right product development people, they would have been stymied by the existing organizational structure, which housed them in tech support, answerable to geographic business leaders whose top priority was wringing profits from existing products rather than investing in risky new offerings.

The lesson from that unfortunate experience is that one of the basic tools of strategic execution is an integrated plan that takes into account the entire organization and provides a detailed blueprint – including a sequenced timeline, clear accountabilities, and a dashboard of key performance metrics – for replacing or reshaping each of the pieces and then putting them all back together. That kind of carefully orchestrated and thoroughly integrated planning is rare. And it's unreasonable to think of these plans as permanent; even as executives are implementing the strategy, conditions change, key people come and go, tactics have to be modified. That's to be expected. But the fact that the process tends to be so fluid underscores the vital importance of a constancy of purpose at the top of the organization.

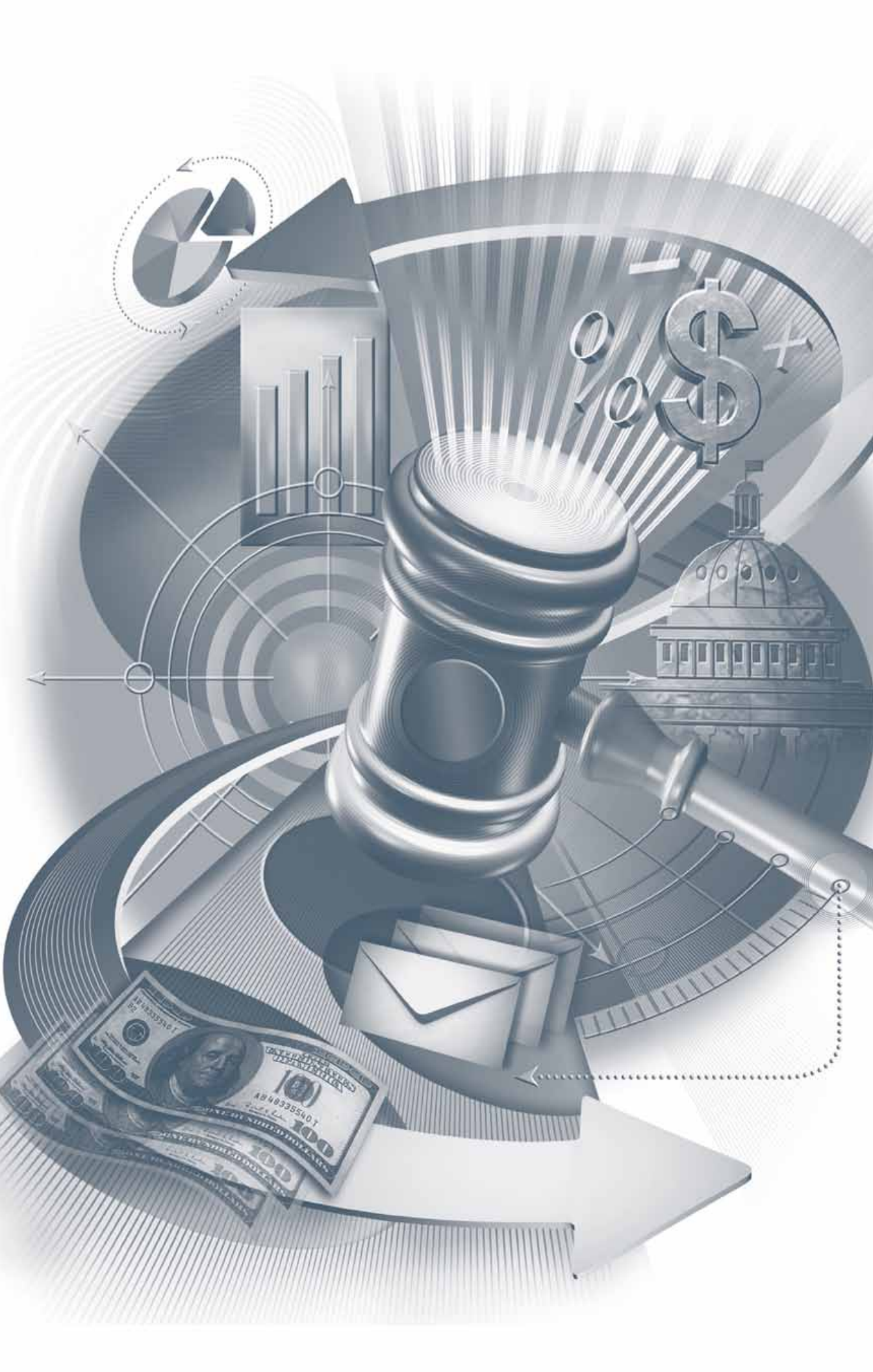
The big unfreeze

The most unsettling aspect of the current economic crisis is that no one seems to have any real idea of how bad it will get or how long it will last. That pervasive uncertainty threatens to create the greatest risk of all – widespread organizational paralysis.

Unfreezing the crisis paralysis will require sound strategies and, even more importantly, effective execution. Attention to operational details is critical, but even more important is an overall sensitivity to the political, emotional, and process dynamics that come into play whenever a major new strategic initiative is set in motion.

Senior leaders need to think about who stands to win or lose from the new strategy, and how they're likely to react. Think about how to translate grand strategy into personal terms that provide individuals with a sense of purpose and some degree of confidence. And think about the ripple effect each action will have across the organization. Trying to assemble isolated pieces of a complex strategy in an organizational vacuum is a sure way to fail – and that's the kind of failure none of our companies can afford today.

Mark Nadler is a Chicago-based partner of Oliver Wyman Delta. He can be reached at mark.nadler@oliverwyman.com.



Combating Pay Equity Risk in a Recharged Climate

Pay Discrimination Suits in a New Era of Federal Scrutiny

As if employers don't have enough to worry about in these unprecedented economic times, they are suddenly exposed to new risks arising from pay discrimination claims. The economic decline in itself, and organizational responses to the decline, are driving discrimination claims to record levels. On top of that, following enactment of the Lilly Ledbetter Fair Pay Act, the Obama administration has stepped up funding for increasing government resources targeted at enforcement of equity laws, and such looming legislation as the Paycheck Fairness Act means that companies that haven't already done so need to take proactive steps to identify and mitigate risks.

*by Michael Burniston &
Brian Levine*

A crucial consequence of the Ledbetter Act – which essentially eliminates the deadline for incumbent employees to file charges of pay discrimination based on race, color, religion, sex, national origin, age or disability – is that it could force employers to defend pay decisions made many years ago. Named for a plant supervisor who sued her employer for alleged pay discrimination, the Ledbetter Act restarts the 180-day



time period (300 days in some states) for filing a charge of discrimination each time an employee receives wages, benefits or compensation negatively affected by an employer's allegedly discriminatory decision or practice, regardless of when that decision or practice occurred. If discrimination is found, each plaintiff is entitled to up to two years back pay. Compensatory and punitive damages also may be awarded in some circumstances. In the context of a class action suit, the potential liability can be very significant.

Meanwhile, the pending Paycheck Fairness Act (PFA) would dramatically increase potential awards for Equal Pay Act (EPA) claims by allowing for uncapped compensatory and punitive damages in addition to the EPA's current remedies of back pay and liquidated damages. The PFA would shift the evidentiary burden from employees to employers, making it considerably more difficult for employers to defend against discrimination claims. It would eliminate the requirement for claimants to provide anecdotal evidence of discrimination and force employers to substantiate legitimate drivers of pay differences. The PFA would also increase the size of class actions by requiring potential plaintiffs to "opt out" of claims, replacing a prior "opt in" standard.

Inherent liabilities

These new realities raise the stakes for employers with respect to various business risks, prime among them litigation risks associated with significant financial exposure. Well before the Ledbetter Act, the Office of Federal Contract Compliance Programs (OFCCP), which enforces affirmative action requirements for federal contractors in the U.S., made compensation assessments a top priority, adopting regression analysis as its new

evaluation standard to increase its effectiveness in seeking out remedies. Further, both the OFCCP and Equal Employment Opportunity Commission (EEOC) have moved to prioritize investigations of systemic risk, which are more likely to lead to class actions. Pay equity enforcement and associated discrimination lawsuits have resulted in hundreds of millions of dollars in agreements and judgments in recent years.

Perhaps more significant than the direct financial exposure is the risk to corporate and product reputations, especially with regard to high-visibility brands, which can be threatened and quickly affected by public reports of workforce unfairness. Bad press can cost a company customers—never a good thing, but especially dangerous at a time such as this, when revenues are threatened by the economic downturn and heightened consumer sensitivity. Pay inequity also can threaten the ability of companies to attract and retain increasingly scarce, diverse talent.

Perhaps the greatest challenge facing employers under the Ledbetter Act is the prospect of having to defend compensation and other employment decisions made so far in the past that documentation, witnesses and relevant decision makers may no longer be available. Other provisions of Ledbetter, however, also create challenges – and risks – for employers. For example, the law potentially expands the pool of potential plaintiffs beyond current and former employees to include “affected” parties (arguably employees’ family members and beneficiaries). It also opens benefit programs to litigation threats due to claims that reduced benefit levels (e.g., pension benefits) were based on discriminatory pay actions made years, even decades, earlier. In addition, the



law specifically states that it applies to a discriminatory compensation decision “or other practice.” Consequently, the law’s reach, ultimately, may extend broadly to cover all manners of workforce practices.

While it’s hard to predict how courts will judge the merits of such actions, or how far back into the past they may reach, the potential for increased litigation requires that employers act now to mitigate risk. That means, on a basic level, spending today’s limited compensation dollars wisely by assessing the match between actual pay practices and compensation philosophy, highlighting cases where pay is out of alignment, and making pay adjustments to limit the ability of employees to credibly raise discrimination claims.

Standards and recommendations

In light of these risks, pay equity assessment needs to be on employers’ 2009 agenda. To make efforts most effective, the approach should be consistent with legal standards of evaluation – in this case, regression analysis.

In 2006, the OFCCP declared regression analysis to be the new standard of statistical assessment for its compensation reviews, moving federal contractors to use that approach to effectively insulate themselves from audit risk. Regression analysis is, in fact, the definitive defense accepted by the courts; in moving to follow the OFCCP’s lead, organizations can more effectively address increasing litigation risk as well. The government’s emphasis on “systemic discrimination” cases also is likely to continue, covering more employees and creating situations that are more likely to lead to class-action suits.

Thus, Mercer recommends that employers conduct regression analyses to find business areas with potential issues, and, within those areas, specific employees for

whom pay changes should be considered. Specific cases for pay changes then should be further investigated and acted upon, as appropriate. To ensure optimal protection in the face of the Ledbetter Act, efforts should be made to level the field on pay, year after year, to make potentially discriminatory past decisions irrelevant. Such analyses can also serve to check rewards-system performance at the aggregate level to ensure that the company is spending its limited compensation dollars as needed to drive company performance objectives.

To further minimize risk, employers need to: implement guidelines for compensation decisions; carefully review and document the basis for pay and promotion decisions to ensure objective support; and train managers and supervisors to clearly define and communicate employee roles, objectives and performance criteria. Employers also should review and potentially revise their document retention policies in order to ensure records supporting past workforce decisions are preserved and readily accessible.

In the course of conducting pay equity assessments, we have found that organizations should keep in mind seven principles to ensure success:

1. Seek the truth

Knowing how the organization will fare in the event of litigation or government audit will allow you to address any existing problems and mitigate related threats. For this reason, the analysis should be conducted with the objective of identifying "systemic" issues.

While the need for apples-to-apples comparison is clear, analyses should not solely focus on job-by-job, location-by-location and/or pay grade-by-pay grade review. Such narrow examination ignores the benefits of statistical

analysis, which can account for multiple differences between employees simultaneously. An effective analysis will balance the need for workforce segmentation against the loss in statistical power to identify key issues. Ultimately, key differences in compensation philosophies across segments should serve to define break points.

2. Don't wait for the data to be perfect

Multiple regression analysis is a starting point. Results are suggestive: they point to areas where action might be critical. Following the analysis, research should be done on pay levels for specific employees.

Because this work is in itself a research process, every element of data available need not be available before moving ahead. Instead of focusing on the impossible task of collecting comprehensive data and/or scrutinizing the validity of data elements across the enterprise, focus on a small subset of the workforce that is revealed to be out of alignment with observed, internal compensation norms.

3. Support – and strengthen – compensation philosophy

In considering adjustments for specific employees who are out of alignment on compensation based on a multiple regression analysis, there is limited potential distortion of the compensation system's intent, provided that the intent matches with actualized practices. What is generally rewarded is simply reinforced, and so the integrity of the compensation system can be strengthened. In contrast, across-the-board changes – based on membership in a protected class, such as increasing pay for all women in a group by 2% – can drastically change relative pay distributions and create inequities.



4. Consider systemic solutions

Multiple regression analysis can also point to specific policy changes to improve pay equity in the long term. Among questions that can be assessed are the following:

- Do pay inequities by gender or ethnicity stem from the point of hire? (If so, target initial pay-setting processes for change.)
- Are full-time equivalent pay differences driven by full-time status and/or past leaves of absence? (Because women are more likely to work part-time and to take leave, gender equity might be at risk.)
- Do pay inequities arise from potential performance-rating bias? (If so, train supervisors to ensure that ratings are fair and that reviews are thoroughly documented and checked.)
- Do promotions into key positions depend upon specific experiences and/or credentials? (If so, ensure that women and minorities have access to such experiences, potentially by providing training; also consider the need for such hurdles for these positions.)



5. Solicit broad support

Various constituents have vested interests in and/or have knowledge that should be brought to bear on proactive pay equity evaluation. For example:

- Senior leadership wants to ensure the integrity of organizational brands, limit financial risk, and enforce organizational diversity and inclusion policies.

- Counsel needs to be consulted to implement the process in a manner that minimizes potential exposure. Together with risk managers, inside counsel can provide guidance on enterprise-wide risks.
- HR and compensation managers can ensure that populations are segmented and models are built to reflect actual rewards policies and practices.
- Employee relations and affirmative action personnel provide critical context and serve to ensure that the evaluation is performed in a manner consistent with related compliance efforts.
- Diversity leaders have a responsibility for programs to increase representation and inclusion. Pay equity is a key condition for success.

6. Ensure neutrality and consistency

Implement a review process that ensures broad workforce coverage and in which all employees have an opportunity to have their own pay levels reviewed: Agree on the level of review (e.g., by business, job family and/or by geography) in advance. Be consistent on employee-level pay change exceptions (e.g., no pay adjustments for poor performers to ensure clear rewards messaging; pay changes to be constrained by the official range for the pay grade).

7. Do good – again and again

Because the workforce is dynamic, with hiring, terminations, promotions, transfers and pay changes, pay equity processes should be ongoing. For federal contractors, annual review is required; however, for nearly all employers, annual review makes sense given the risks and associated benefits of the effort. Optimally, the review should coincide with the annual compensation evaluation process. Sudden, even planned, changes to the workforce

and related pay programs – in the face of the economic recession and business climate – could easily disrupt and change a seemingly strong pay equity position.

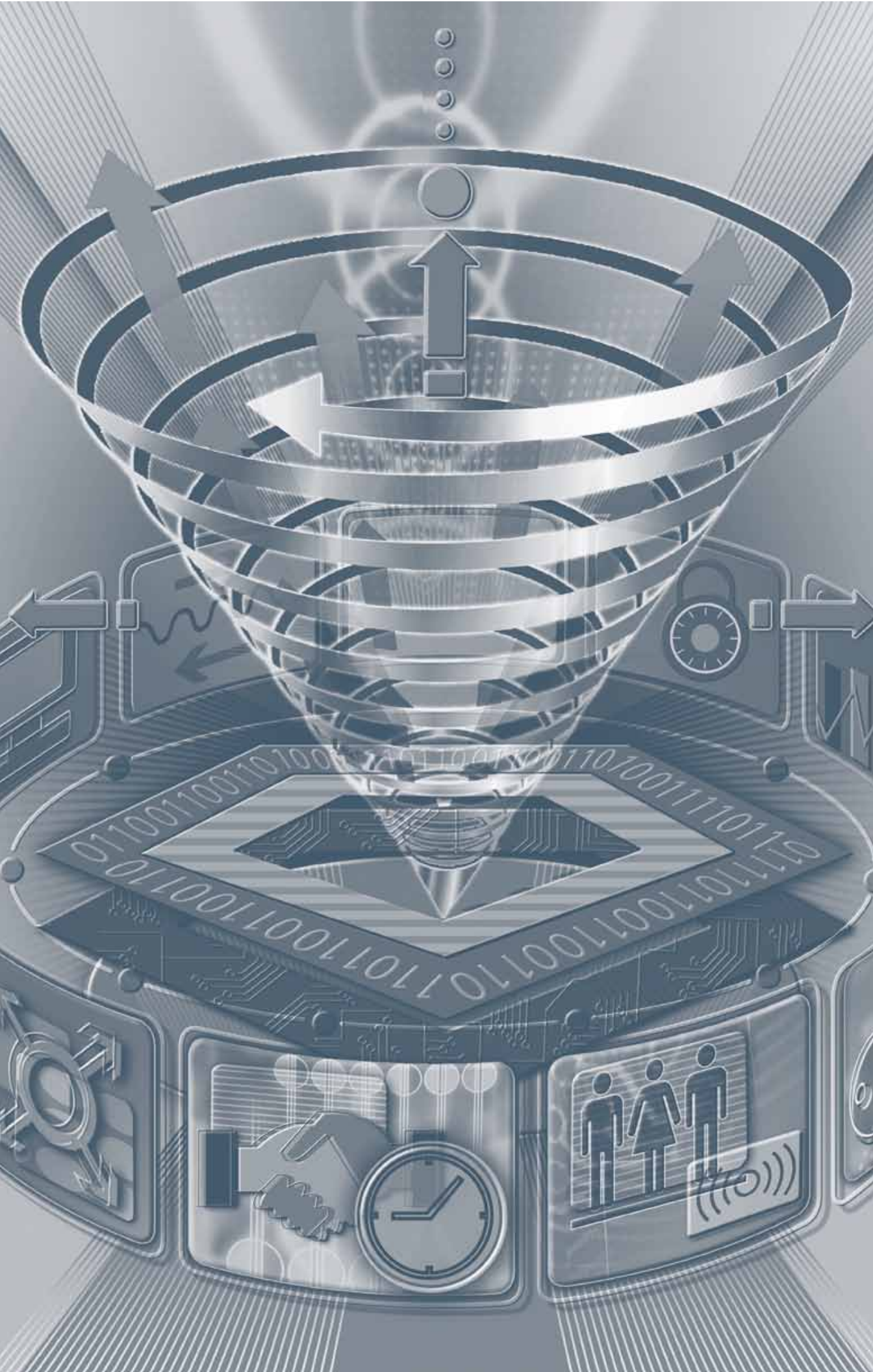
Summary

In the face of the Ledbetter Act explicitly, it is important to reduce the risk that a claim will be made based upon past actions. In correctly structuring pay equity analysis now, one can ensure that everyone's pay is in line with norms generated on an appropriate basis. As a result, differences based upon past, now irrelevant decisions will be reduced over time, as will potential claims and threats to your organization's brands and reputation. Indeed, proactive assessment is like insurance: a small premium – in terms of dollars and effort – can serve to mitigate significant risk.

Michael Burniston is the New York-based leader of Mercer's Human Capital business for the U.S. region. He can be reached at michael.burniston@mercer.com.

Brian Levine, PhD, is a New York-based principal in Mercer's Human Capital business and is the firm's lead advisor to clients on matters pertaining to pay equity. He can be reached at brian.levine@mercer.com.

To learn more about the implications of the Lilly Ledbetter Fair Pay Act, its potential impact and how to take appropriate action in response, please visit <http://www.mercer.com/rewardsfairness>.



Confronting Fraud in a Downturn

Old Scams and Evolving Risks

The global economic downturn and uncertainty in market conditions have created an environment that both exposes existing financial scams and engenders new frauds.

*by Richard Abbey, Alan E. Brill &
Brian G. Lapidus*

With banner headlines publicizing massive frauds around the world, individuals and businesses are paying increased attention not only to investments but also to questionable operations. Swindles that rely on a continuous supply of new victims are harder now; people have less money to invest and often switch to safer investments. Furthermore, companies watching costs are more likely to investigate unusual spending. As old frauds come to light and regulatory bodies inevitably take action, businesses can benefit by anticipating and preparing for the consequences.

At the same time, increased competition for fewer opportunities is straining ethical boundaries. Economic difficulties can change the behaviors of normally trustworthy people. Some individuals facing intense financial pressure will resort to crime, driven by desperation or unwillingness to make lifestyle adjustments.

Those with responsibility for a company's finances may be tempted to become "corporate saviors," massaging figures in a misguided attempt to save a struggling business. They may conceal the company's true financial position in order to prevent staff reductions, cover up breaches of banking covenants, obtain credit from suppliers, or raise new debt or equity. Often these individuals believe that falsifying financial statements will be only a temporary measure until business improves. Frequently, however, the fraud has to grow as the company continues to lose money.

As businesses deal with the difficult decision to reduce staff headcount, employee morale and data security must be addressed. Employees who feel slighted may be more tempted to misappropriate intellectual property or personal information from employees or customers. Tightening budgets are causing some companies to cut back on data security measures, even though proprietary data and personal information is at increased risk.



Regardless of the motivation for fraud, companies must consider how to protect themselves, how to detect and investigate malfeasance, and the regulatory obligations that arise.

Preventing fraud

Enhanced due diligence

Institutional and private investors alike have been shocked to discover that they have been duped by trusted professionals with strong track records. Thorough investment due diligence is important; however, it is only one aspect of comprehensive fraud risk management. A broad approach to due diligence – rather than a “check-the-box” review – is not only vital to managing risks through the economic downturn, it greatly assists effective day-to-day business operation. Businesses must ensure that they have sufficient knowledge about prospective employees, business partners, third parties, and transactions.

With economic distress contributing to business closures and job loss, ensuring the authenticity and integrity of front-line employees and executive leadership is critical. As always, new applicants should be screened to verify identity and work history claims, as well as to discover any criminal record that might block employment. Ongoing screening at achievement points (promotion, additional access to confidential information, etc.) or at timed intervals will decrease the potential for a new risk to arise and remain undetected.

Components of partner relationships and transactions, such as individual employees, principals, and business entities, require analysis to prevent possible negative effects on revenues or reputation. Businesses should not feel safer in certain countries; this is a global issue relevant to all industries. International due diligence can



be challenging, but need not deter investments abroad or entry into new markets. Comprehensive, compliance-driven investigations can provide crucial information on important decisions, providing lasting business benefits.

Finally, businesses must screen third parties who will work on company property, alongside personnel or directly with clients. It is not unreasonable to expect vendors to mirror the company's existing screening standards, providing an extra layer of protection from possible risk.

Monitoring and corporate governance

Internal controls, no matter how good on paper, will be ineffective if improperly implemented or monitored, or if collusion within an organization allows them to be bypassed. Supervision is fundamental to reducing opportunities for dishonest behavior and ensuring that possible fraud is flagged early. Those responsible for managing fraud risks must thoroughly understand the business and its people, particularly in overseas or remote locations. Companies looking to shave costs on international operations must also be prepared to understand developments in the supply chain and how that may affect the business. For example:

- Senior executives must have a practical, hands-on understanding of how each division, as well as the company as a whole, makes money. A solely theoretical perspective may leave gaps in understanding whether reported revenues logically follow from the business activities.

- Risk managers, compliance teams, and non-executive directors should understand whether the profits align with trends in the global economy. They should ask questions such as: Why are we the only company in our sector generating such high/low returns? And, why does this star performer complain about internal audits? Red flags must not be ignored for fear of upsetting sales teams or senior management. While executives face constant pressure to generate increased profits, an overlooked fraud will be significantly more expensive in the long term.
- Financial institutions must ask: Do our senior managers and auditors really understand the products that are being traded and the attendant risks? In financial organizations, there is a great deal of scope for improper disclosure and misrepresentation. Trading products are highly sophisticated and often senior managers are not trained to use the technology, therefore relying on the knowledge of junior staff.

The economic downturn will also lead to tighter regulation. In the United States, for example, the Securities and Exchange Commission announced earlier this year that it will be increasing the severity of penalties it seeks for Foreign Corrupt Practices Act (FCPA) violations. The impact of an investigation – including legal costs, potential fines, and negative impact on market capitalization or reputation, can be devastating. Those contemplating foreign activity must therefore ensure that they take an FCPA-compliant approach, which includes: maintaining and adhering to



written policies and procedures, using risk-based metrics to determine the depth of the due diligence investigation, and engaging specialists to help obtain the information necessary to understand business operations fully.

Responding to fraud

Whistleblowers, investigation and forensics

The vast majority of fraudulent activity is uncovered by accident or through whistleblowers. Companies, therefore, must have an adequate framework to handle whistleblowers both internally and externally. They must investigate reports of unethical or fraudulent activity, clearly document how allegations were addressed, and create a summary of the outcome.

When a potential incident occurs, an internal investigation becomes necessary. The first order of business is to create an investigative team that includes counsel, a forensic accountant, and an investigator. The right investigator is often critical, requiring a combination of experience in the relevant kind of fraud investigation and a thorough understanding of the facts of the case. Additionally, most internal investigations will require computer analysis; if an investigation involves data collection and/or analysis, the investigator must have experience in proper forensic protocols.

Once formed, the team must quickly determine the likely key issues, and create a data map outlining the location of all potentially relevant information. This will also involve identifying key custodians of the data and how the company normally conducts business related to the

fraudulent activity. Evidence must be preserved in a way that protects its origin, integrity, and chain of custody. Preservation is often complicated by the involvement of personal computers or other types of electronic storage. Investigators must secure data from all sources in a defensible manner following proper forensic protocols in order to avoid tampering claims.

Interviews are often an essential part of a fraud investigation, but before proceeding the team should construct a timeline detailing the evidence and suspected players. This will provide a clearer understanding of what may have happened and permit more efficient questioning during interviews. Where relevant in the interviews, investigators should use information gained throughout the investigation to ask pointed questions, properly gauge answers, and establish if a witness is being untruthful or obstructive.

Applying best practices is vital in conducting a successful investigation into allegations of fraud. A sophisticated investigative team can increase a company's chances of determining who was involved in the fraud, giving a company a heightened chance to regain a portion of the losses and prevent future incidents of fraud.

Data breach notification

When a fraud includes a breach of sensitive personal data – of employees, customers, or other constituents – a whole new audience demands attention. The response must be deliberate and prudent. An Incident Response Plan (IRP) should, among other things, identify an internal



team to manage the event, as well as establish a chain-of-command for investigation, assessment, and notification of required agencies and impacted individuals. The company should also preselect identity management products and services that can be deployed quickly to help those affected recover their pre-breach status and confidence.

Complying with diverse legislative requirements can be daunting. For example, one law might call for a detailed description of the event while another might simply require an approximate date of discovery. Few organizations face data breaches daily. It may be useful to engage an outside specialist with up-to-date knowledge of, and a proven record in, this complex area. Depending on the size, type and visibility of the organization, the IRP team might also benefit from crisis communications practitioners, to counsel team members and oversee the release of information to media and industry observers. Reputational recovery requires a concentrated effort to assure internal and external onlookers that the incident has been addressed, and all reasonable measures have been taken to halt further damage.

Looking ahead

Corporate in-house and outside counsel are expected to be kept busy for the next few years as investigations and legal claims rise sharply. Companies need to focus not only on the immediate situation, but also on the likely long-term effects. If history is any guide, companies will see a substantial increase in fraud claims, legal disputes and regulatory actions. With increased litigation comes increasing data retention requirements.

Over the coming months and years, new regulations will likely be imposed on these companies, placing a bigger burden on already strained budgets and resources. Additionally, the majority of modern litigation involves at least a minimal amount of electronic discovery. Taking a proactive approach is vital. Pertinent members of the company's response team should know where data is kept and how it is maintained. Keeping communication lines open is also important to ensure everyone in the company remains on the same page. This will allow a more efficient and well-educated response to any legal discovery requests, audits or regulatory compliance requirements, which will ultimately help save time and money.

The economic downturn has brought old frauds to light and created an environment in which new risks can evolve. In these uncertain times, businesses must know where vulnerabilities lie, be prepared, and plan their responses accordingly.

Richard Abbey is a London-based managing director of Financial Investigations at Kroll. He can be reached at rabbey@kroll.com.

Alan E. Brill, CISSP, CFE, CIFI, is a New York-based senior managing director of Computer Forensics at Kroll. His email is abrill@krollontrack.com.

Brian G. Lapidus is the Nashville-based COO of Fraud Solutions at Kroll. He can be reached at blapidus@kroll.com.

Enterprise Risk Management Did Not Fail in 2008

Look Deeper for the Underlying Causes

The profound financial damage that began last year has left the insurance industry looking for answers. Diligent underwriting and conservative investment strategies were not enough to prevent natural and financial catastrophes from bleeding balance sheets. Both leadership teams and key stakeholders have questioned the value of Enterprise Risk Management (ERM) frameworks, yet the conclusion that ERM failed may be hasty. After all, the insurance industry actually survived the events of 2008 reasonably well, with at least some of the credit going to their ERM efforts. Where risk management did fail, the underlying causes were deeper.

by Donald Mango

Models and ERM frameworks alone cannot protect capital from the myriad threats that carriers face. They will never replace the judgment, insights and decisions of risk management professionals. As we look forward to the balance of 2009 – and well into 2010 – the insurance industry should reflect on the lessons of last year and plan their ongoing ERM investments accordingly.

A year of significant loss

The insurance industry faced both natural and financial catastrophes in 2008, causing a spike in insured losses and depleting carrier investment assets. Both sides of the balance sheet were subjected to incredible pressure. The insurance industry spent six months revising estimates from Hurricanes Gustav and Ike upward, while the ultimate tally of investment losses from the financial crisis continued to climb. Insured losses were much higher than anticipated, and carriers have struggled to replace even a portion of the capital consumed by these events.



The net effect was an 18% drop in reinsurers' shareholders' equity, as measured by the Guy Carpenter Global Reinsurance Composite. While a handful of carriers were able to protect (and even increase) their capital, most were down, with a few losing 40% or more. Of course, the situation was much worse for the broader financial services industry, particularly the banking sector. In addition to losing shareholders' equity of more than 30% on average (which includes the effects of the Troubled Assets Relief Program), several global banks with robust balance sheets, long operating histories and unassailable reputations disappeared.

In contrast to the banking sector, the non-life insurance industry fared relatively well. There were a few high-profile casualties in the life insurance sector, but the losses were attributable to asset linked insurance and annuity products. Conservative accounting and risk management practices contributed to this relative success, but another key factor was the sizeable capital cushion with which carriers entered 2008. In fact, the most common conversation among insurance industry leaders at the start of 2008 involved how to make excess capital productive. Dividends were routine, and share buybacks abounded. Even with the aggressive return of capital to investors, carriers still generally had robust balance sheets, which helped them absorb the effects of a perilous September.



Nonetheless, it's difficult to keep this perspective when staring at a much leaner balance sheet. Whether it is pessimistically called blame or perceived as an opportunity to improve, carriers have fervently sought answers. For many, the buck stops at ERM.

Expectations and ERM

Did ERM work: yes or no? Opponents argue that this supposedly advanced thinking on the management of capital failed to keep balance sheets healthy throughout the economic crisis. Insurers losing more than 30% of their capital cannot be faulted for concluding that ERM did indeed fail. Alternatively, supporters point out that the capital was depleted because it absorbed unexpected loss – arguably a core function of insurer capital. The holistic approach to risk management meant insurers were beaten but not broken.

The difference is one of expectations, and the truth is somewhere in the middle. Those who expected ERM to provide a comprehensive, impenetrable safeguard were disappointed, while carriers seeing their frameworks as having repelled an assault on their balance sheets claim success.

In either case, there remains room for improvement. Insurers withstood a major test of their risk management capabilities, and should find ways to strengthen their ERM frameworks. The conditions for self-examination are ideal; We are looking back on the unimaginable with the benefit of some painfully earned experience. Furthermore, capital remains constrained this year, requiring companies to exercise risk management discipline in their portfolio planning.

Managing constrained capital

Going forward, the insurance industry will have to change its thinking. The crutch of excess capital has been kicked from beneath the industry's arm. Despite some recent successes in capital raising, the largesse of 2007 and 2008 is unlikely to return in the near future. The insurance industry began 2009 with sufficient capital to bear risk and operate without fear of insolvency, but the coffers were lighter than the year before. The industry is bruised and may not be able to absorb a reprise of the realized risks of 2008. A new approach to managing and measuring risk is necessary, one that addresses the full spectrum of threats that carriers face.

This implies a profound shift in how carriers understand, price and monitor risk. No exposure exists in a vacuum, as a single event could affect many lines of business or insureds. Companies need to develop their scenario modeling capabilities. This will require a degree of structured creative thinking among the management team and key opinion leaders. Last year, few accounted for the fact that a devastating hurricane would strike Galveston, Texas as a financial catastrophe shook New York, London, Hong Kong, and other money centers. Firms must start by conceiving of the scenarios that could impair balance sheets, but they must follow that with an assessment of the impact of those scenarios, as well as the projected effects of any mitigation steps. Most insurers have found the best way to do this is an internal risk and capital model.

Guy Carpenter's MetaRisk® model, for example, enables risk managers to evaluate all major risk sources: underwriting, reserving, catastrophe, credit, market, and operational. The model supports a holistic approach to risk by capturing the risk characteristics and interaction effects in one master file – thereby becoming the official risk record of the company. Once the range of impacts has been quantified, corporate risk tolerance levels can be matched with reinsurance coverage and other hedging strategies to demonstrate to stakeholders how, under a host of possible scenarios, the company's risk and capital management plan preserves the franchise.

It is important to stress that even the most advanced risk technology cannot replace the human element in risk decision processes. In fact, one could argue that over-reliance on automated logic materially contributed to the financial catastrophe in which the market is currently mired. Instead, think of this technology as facilitating the development of a risk management competency in these organizations – the emergence of a new breed of risk professional, able to use these tools, along with knowledge of the business dynamics and drivers, to provide a company's leadership with expert navigational guidance.

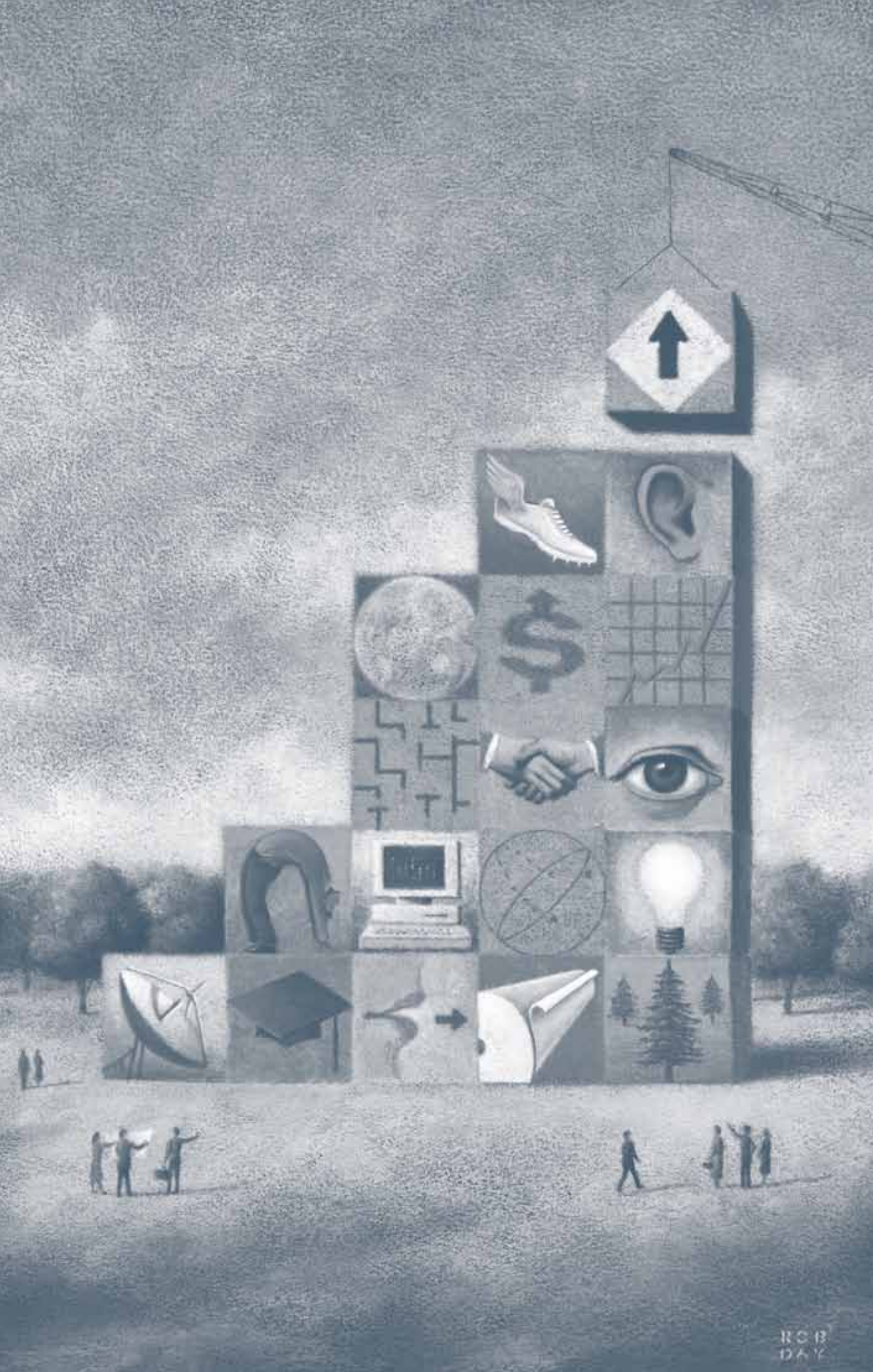
The road ahead

Fragmented risk management approaches are no longer viable. Threats are too systemic and pervasive to be effectively managed from silos. The world has learned an enduring lesson from the crisis of 2008: a convergence of threats, perceived or otherwise, can impair an entire industry or even economy.

In past years, the insurance industry could turn to a number of capital sources in a post-catastrophe year and restore balance sheets. In 2009, this tactic is unlikely to be effective, as the supply of capital has dwindled and the cost has increased. Instead of merely reloading on capital, the insurance industry will have to focus on making better use of the capital they have.

The key to making the most of the capital that carriers have on hand will be the adoption of an enterprise-wide understanding of risk, as well as the tools to manage capital based on the full spectrum of risks. ERM, once considered an opportunity to sustain a competitive advantage, is likely to become part of the price of admission to the insurance space.

Donald Mango is chief actuary of Guy Carpenter & Co. He can be reached at donald.mango@guycarp.com.



Risk Management and Economic Change

A Catalyst for Re-evaluating Business Preparedness, Mitigation and Response

When the economy changes, business priorities and perspectives must also change. This is not only crucial to survive, but to persevere. Maintaining liquidity might seem like the most important organizational priority; however, a company needs to fortify itself against ongoing disruptions, such as the loss of critical infrastructure as well as the fallout from initial change. Putting risk management aside while tending to “daily survival” is expected, but organizations need to realize that other disruptions are inevitable and economic volatility increases the chances of an adverse event occurring.

by Gary S. Lynch

The goal of risk management is to minimize an organization's exposure and to keep the business running smoothly during disruptive situations. What could be more unsettling than the failure of business partners, deterioration in quality standards, consolidation of facilities, loss of corporate memory via reductions in the workforce, and offloading assets – all symptoms of changing economic times?

Change has been thrust upon us – industry change, business change, supply chain network change, operational change, third-party relationship change, even change in



customer demand. These changes have put a company's preparedness, mitigation and response capabilities at risk – and in worst cases, made them obsolete.

Warning lights that change was imminent were flashing in boardrooms around the world as demand rapidly declined, trade credit tightened, and suppliers ran out of cash. For example, the continuity of the textile industry supply chain was impacted when the number of suppliers rapidly shrunk from 22,099 in July 2008 to 6,262 in October 2008 – a reduction of 72%.¹ As a result, composition of the supplier base varied, configuration of warehouses in relation to customers was altered, and inventory levels decreased throughout the supply chain. This directly impacted existing preparedness, mitigation and response strategies.

Though change surrounds us, the expectations of a company's customers, investors, business partners or regulators do not change. Businesses are still accountable for providing value to the market and maintaining the ongoing entity during adverse times. There is no excuse for ignoring sound and proven risk management practices just because economic times are tough. And auditors, rating agencies, regulators, and other external parties that measure an organization's risk management practices can add fuel to the fire by offering a negative opinion that translates into a greater cost of capital or worse – negative press. Who wants to do business with a seemingly risky company?

To counteract the potential threat of obsolete or ineffective continuity risk management programs, organizations must move quickly and efficiently. All organizations should consider whether they are actively engaged in the change as it occurs for the purpose of understanding

¹ Panjiva, a company that collects and disseminates data on global suppliers and manufacturers (<http://panjiva.com/>).

what products and services are considered of greatest value. Businesses should ask if these changes have been documented and validated by executive management.

A company must understand its business operations, its supply chain interdependencies, and the final configuration of its processes and resources as a result of change – in people, technology, physical assets or relationships. Companies need to move beyond continuity risk management focusing on a facility or function to an approach that begins with value and processes. The goal should be to align risk investments against that which could have the greatest impact to the value produced by the organization. This is an economic exercise, where businesses should try to do the most with the least: in other words, understanding that there will be a finite amount of available risk capital, time, resources and management bandwidth.

How to plan, mitigate and respond

Organizations should expand the scope of their planning activities to take into account the potential effects of change.

- Planning should include the extended operation and third parties – from raw materials through supplies and logistics providers to the final customer.
- The mitigation strategy should include the strategic design layer (warehouses, factories, and supplier locations) or the day-to-day operations (transportation, inventory management and production scheduling).



- The preparedness, mitigation and response capabilities should include:
 - what is of greatest value to the organization (value segmentation and the priorities of the organization);
 - the resources and processes that are needed to support the creation, delivery, and servicing of value (process and resource mapping);
 - the quantifiable and qualitative impact from loss of a critical resource, according to value – revenue, assets, liquidity, strategic, brand/confidence, and compliance;
 - analysis of the required risk investments compared to potential impacts (risk financing/insurance, retention, or retention with mitigation); and
 - validation of the risk mitigation (test, audit and simulation), monitoring of the environment, and assessing and optimizing risk solutions continuously.



An organization should also have preparedness, mitigation and response plans in place and updated regularly to reflect changes such as: the consolidation of warehouses or the shutdown of a plant, elimination of suppliers, decreased inventory levels or new transportation carriers, and, most importantly, have those organizations they rely on understand and meet their expectations.

And when there's disruption...

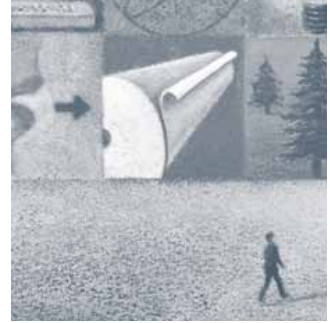
At the time of disruption, the goal becomes to minimize the financial and brand impact by utilizing information gathered prior to the disruption on the potential effect on the organization's failed resources.

A company's preparedness, mitigation and response programs should contain event identification, including criteria for recognizing and responding to an event, which, if determined, will activate incident/emergency plans, such as evacuation and life safety, product tampering, civil disturbance/terrorism, or contractor contingency procedures. The response programs should have as their primary focus ensuring the survivability of the organization as well as a clear direction and communication with key stakeholders.

Containment should be determined if the desired impact thresholds and recovery times will be exceeded. Escalation should be based on predefined protocols and thresholds for escalating or promoting information and news flows in a timely, relevant, consistent, and accurate manner. There should be a clearly defined path for information among all stakeholders.

During post-disruption, organizations should conduct a postmortem review of lessons learned, focusing on questions such as how the organization improved its risk mitigation and financing activities as a result of the event; what problems were encountered; was the response effective; was the impact contained from the event; and if not, was the organization able to recover, restore and resume normal operations.

In changing economic times, assumptions may be altered, but it is clear that expectations are greater as organizations experience more volatility and stakeholders require greater diligence. Failure to align with these expectations could be interpreted as a failure to exercise proper governance and due care – putting everyone at risk.



Gary S. Lynch, CISSP, is a managing director in the Supply Chain Risk Management Practice of Marsh Risk Consulting. He is the author of *At Your Own Risk*, Wiley, 2008, and of the forthcoming *Single Point of Failure – The Ten Essential Laws of Supply Chain Risk Management*, to be published by Wiley. Mr. Lynch can be reached at gary.lynch@marsh.com.

Viewpoint

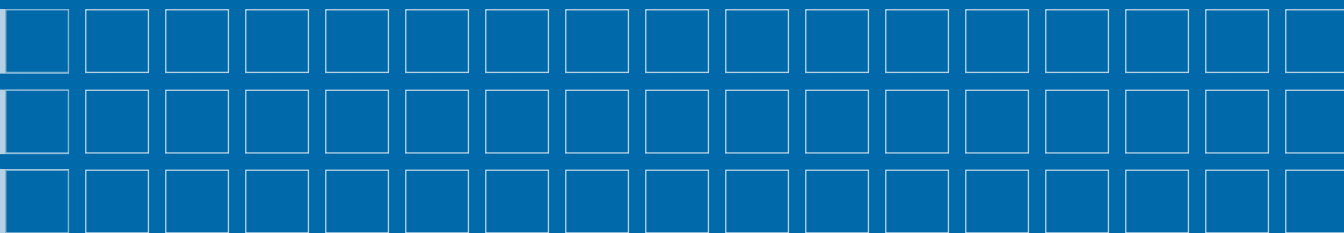
As the name *Viewpoint* implies, the articles in this journal represent the ideas and opinions of various employees of Marsh & McLennan Companies (MMC) and others. The articles do not necessarily represent a consensus of company thought on any subject.

MMC is a global professional services firm providing advice and solutions in the areas of risk, strategy and human capital. It is the parent company of a number of the world's leading risk experts and specialty consultants, including Marsh, the insurance broker and risk advisor; Guy Carpenter, the risk and reinsurance specialist; Kroll, the risk consulting firm; Mercer, the provider of HR and related financial advice and services; and Oliver Wyman, the management consultancy.

Approximately 53,000 employees provide analysis, advice and transactional capabilities to clients in 100-plus countries. Its stock (ticker symbol: MMC) is listed on the New York, Chicago, and London stock exchanges. MMC's website is located at www.mmc.com.

To learn more about MMC and our subsidiaries,
visit the following websites.

Marsh & McLennan Companies	www.mmc.com
Marsh	www.marsh.com
Guy Carpenter & Company	www.guycarp.com
Kroll	www.kroll.com
Mercer	www.mercer.com
Oliver Wyman	www.oliverwyman.com
Lippincott	www.lippincott.com
NERA Economic Consulting	www.nera.com



Viewpoint
Issue 2 2009

Copyright 2009

All rights reserved

