

# Addressing Enterprise Security Risks

By Hal Shear

Reprinted from Directors Monthly with permission of the publisher.  
© 2007 National Association of Corporate Directors (NACD)  
1133 21st Street, NW  
Suite 700  
Washington, D.C. 20036  
202-775-0509  
www.nacdonline.org

Boards have an important role in a successful enterprise risk management program—a role that includes providing oversight, keeping informed of the most significant risks, and understanding the extent to which management has instituted good policies and practices. Since the passage of the Sarbanes-Oxley Act of 2002, public company boards have given increased time and attention to the risk of financial fraud and its prevention. But do today’s boards spend enough time thinking about other types of strategic risk?

In June and early July 2007, I informally surveyed a group of more than 70 people—primarily public company directors, as well as a few content experts and academic researchers. I asked them an open-ended question about what other types of risks—besides Section 404/financial-compliance risks—they think boards should be spending more time on. Thirty people responded, and while the group is not the kind of random sample used to generate statistically valid conclusions, the results shed light on some interesting themes.

Though individual responses varied widely, the directors and experts as a group identified not only market risks—such as those related to strategy, competition, and technology-driven change (the three most common answer categories)—but they also frequently noted various types of security risks related to external events. These included the risk of a terrorist attack; IT and IT security risks; the risk of a natural disaster; supply-chain risk; and more generally, crisis management and preparation.

**Director Summary:** Do today’s boards spend enough time thinking about non-financial risks? Based on an informal survey of directors and experts, the author discusses the board’s role in overseeing the often-overlooked aspects of enterprise risk management, including the risks associated with supply chains, natural disasters, terrorist attacks, and technology.

## Risk of Terrorist Attack

What should boards do to ensure that their companies are adequately prepared for security risks? Consider, for example, the risk of a terrorist attack. According to a U.S. intelligence report released in July 2007, the U.S. is in a “heightened threat environment.” For companies whose locations or operations place them at greater risk of facing the effects of a terrorist attack, boards might ask the following questions:

- Is the company adequately prepared for such an event?
- Is the company prepared for immediate action if operations are affected?
- Is there some level of insurance available to the company for such events?
- Are the lines of authority within the company absolutely clear?
- Are roles defined according to who is going to take what actions in such a situation? Does this include the role of the board?
- If the CEO is not at headquarters when the attack occurs, is the company’s chain of command clear to the board?
- Has everything that can be thought through in advance been thought through?

## IT Security Risks

Another key enterprise security risk lies in the area of information technology and the company’s use of the Internet. This could potentially overlap with the risk of terrorism—as the President’s Information Technology Advisory Committee cited in a 2005 report on cyber security, “the information technology (IT) infrastructure of the United States...is highly vulnerable to terrorist and criminal attacks.” Board members should ask questions about the company’s preparedness for an IT security incident, including:

- Does the company have appropriate redundancy policies for websites and data?
- Does the IT staff constantly seek, through their own efforts or through those of hired third parties, to penetrate the company’s own security defenses?



- Does the company's IT function have the necessary sophistication to monitor potential threats on an ongoing basis?

[Ed. Note: NACD's newest publication, Information Security Oversight, releases this month. See [www.nacdonline.org/publications](http://www.nacdonline.org/publications).]

### Risk of Natural Disaster

As events such as Hurricane Katrina have demonstrated all too clearly in recent years, natural disasters can have devastating effects on the communities in which they occur and the businesses that operate in those communities. What's more, some scientists believe that one effect of climate change and global warming may be more extreme weather events—potentially making the importance of being prepared for a natural disaster even more crucial in coming years. Board members should ask questions regarding the company's level of disaster preparedness:

- Does the company have a plan to protect its employees and facilities in the event of a disaster?
- Are there backup plans? Are they fully developed and tested on a regular basis?
- Is the board involved in reviewing the design and monitoring of those plans?

### Supply Chain Risk

Finally, there is the issue of supply-chain risk—an important yet sometimes overlooked issue. Global supply chains may have many benefits for companies, such as increased flexibility and cost savings, but they also bring concomitant risk. One risk that has been in the news this year involves product quality control—with headlines featuring adulterated Chinese pet food products and other quality control incidents.

There is virtually no company today that isn't at risk in some way from a supplier overseas. As MIT Professor Yossi Sheffi notes in his book, *The Resilient Enterprise: Overcoming Vulnerability for Competitive Advantage*, globalization has led to complex supply chains, and given this complexity, "the number of possible disruptions to a global supply chain is endless." Where once companies need merely be concerned about, say, an earthquake occurring near the location of a company plants, today an earthquake thousands of miles away—but near suppliers' plants—may cause a disruption to operations. The more complex the supply chain, the greater the inherent exposure to risks of all types.

In *The Resilient Enterprise*, Sheffi gives an example of an enterprise risk management team at General Motors, which shared with GM managers a list of "rare events" that might disrupt operations in the company's supply chain—and discovered that virtually every event on the

list had affected GM in the prior 12 months. Sheffi explains in his book that this was not bad luck on GM's part, but rather a function of the company's vast and complex supply chain. He writes that "while the likelihood for any one event that would have an impact on any one facility or supplier is small, the collective chance that some part of the supply chain will face some type of disruption is high."

Clearly, the issue of supply-chain risk is one that needs consideration on a strategic level. As Sheffi and James B. Rice Jr. note in an article in the Fall 2005 *MIT Sloan Management Review*, "building a resilient enterprise should be a *strategic* initiative that changes the way a company operates and that increases its competitiveness." And that means it's an area boards should care about.

From a strategic standpoint, supply-chain risk is an area where boards can add considerable value. As Luke Ritter, principal of Trident Global Partners, noted during a personal interview, "Corporate boards currently have unprecedented opportunities to create value by endorsing and encouraging supply chain initiatives that enhance enterprise security and resilience." In particular, in his book *Securing Global Transportation Networks: A Total Security Management Approach*, Ritter and his coauthors argue that companies need to take an approach to supply chain security that is analogous to a total quality management approach. That is, improving security needs to be seen as a key business function that can create value through a variety of means, including better disaster preparedness or improved brand equity.

### Crisis Management and Preparation

More generally, boards should make security risks part of their strategic discussion. Getting outside assessments of all major risk points—of what you're doing and how well you're doing it—can be quite helpful. At the boardroom level, create a security risk dashboard so the board can monitor how well the company is handling security issues on an ongoing basis. While the implementation of risk assessment and risk management is a task for management, boards that are truly a strategic asset to the companies they serve need to understand the risks those companies face, both in the marketplace and beyond. ■

**Hal Shear** is managing director of Board Assets, Inc., director of e-tractions, Inc., PowerSkills, Inc., Bioethics-in-Action, Inc., and chair of VisionWorkshops, Inc., and GrayDome, Inc.



## Survey Responses: Non-Financial Risks and the Board

*“What risk factors—beyond Section 404/financial-type compliance—should today’s corporate boards devote more time and attention to?”*

*That question was posed to a number of thoughtful and informed corporate directors and other experts in June of 2007. The following are a few samples from their responses.*

### **Jeff M. Spivey** **Chairman, ASIS International**

After Sarbanes-Oxley and other recent legislation, corporate boards are taking an active role in better understanding their business exposure to *all* risks. These risks extend into not only identifying and managing singular risks, but the management of integrated risks that may have significant impact. In recent years, an evolution into more holistic approaches to managing risks for *all* stakeholders has matured. Enterprise risk management models explore the importance of risk-bearing capital analysis, transparency, monitoring of significant risks, setting risk limits, and operating risk management programs that will maintain a consistent level of risk retention for the company by transferring risk through insurance or other contractual agreements. This approach helps to provide consistency across all risks, with the fundamental objectives of the enterprise at the heart of the programs.

Outsourcing presents a new degree of risk that has either been ignored or misunderstood for years. The business case for outsourcing can be attractive, but *all* stakeholders, including all partners outside the company, have to be a part of managing risks and collectively arriving at a holistic risk management program. Risk management as a discipline has been misunderstood as an insurance arm of the company when, in fact, it should be considered as the strongest and most significant process a company and the board has to assure that company risks are properly being managed.

### **Thomas G. Plaskett** **Chairman, Fox Run Capital Associates, Novell, Inc., and Platinum Research Organization, Inc.;** **Director, Radio Shack and Alcon, Inc.**

There is a wide spectrum of board approaches to the topic of risk assessments, which ranges from an annual review of risk, usually at the audit committee level, to a full-blown formal ERM (Enterprise Risk Management) program.

And there is a lot of territory in between, such as a focus on the top five external risks, the top five external and top five internal risks, etc. At the “short end” of the spectrum, the audit committee generally deals more with insurance

coverage adequacy than with overall risk assessment across strategic landscapes, markets, and environmental/external factors.

I believe 9/11 sounded a wake-up call in this area, as many firms found that the impact of such an event tested the adequacy of corporate preparation and programs to handle a crisis. Boards discussed and reviewed the adequacy of assessment, expectations, and preparedness planning. In fact, much of the enterprise risk management program momentum has developed only in the last few years.

I do think there is no single answer to best practice in this area. One size does not fit all. One firm may have as its worst nightmare a product recall or public health crisis, while others may have a technology failure or intellectual property crisis. So at a minimum, I think directors and boards should strike a moderate approach and review the most significant risks across strategic landscapes, markets, environmental/external factors, and internal systems and processes. The risks should be catalogued, researched with impact assessments, and balanced, with risk mitigation plans in place. The board’s principal responsibility is to be assured that management has thought about or assessed the relative risks to the company and has put in place plans to mitigate or deal with a crisis when, and if, it occurs.

### **David B. Winder** **Chair, NACD Utah Chapter; Director, ALSCO, Inc.**

Boards are getting a pretty good handle on internal controls of all types, most of which fit neatly within the jurisdiction of committees that every board has. What concerns me most is external risks that, at least in the early stages, might go unnoticed.

As examples: How many companies fully recognized the implications of globalization and climate change in the early stages? Are most companies, even with the examples of 9/11 and Katrina, making adequate plans to minimize potential damages from natural disasters and terrorist attacks? Are their boards taking an active role in providing oversight to these plans? Perhaps more important, are boards overseeing rigorous activity of management to discern whether all serious potential risks are being assessed, so that the company is never blindsided? Such risk could be not knowing until too late that the research and development department is being outflanked by a competitor, or that a group of disgruntled employees are about to leave and form their own company or join a competitor—and the list could go on and on. I have the feeling that boards are often not focused on these types of risks, and they sometimes assume that the audit commit-



tee or someone in management is taking care of things when they really are not.

**Professor Steve Currall**  
**Corporate Governance Researcher, University College London and London Business School**

Risk assessment by corporate boards of directors must include two key themes relating to the rise of the “BRIC” countries, namely, Brazil, Russia, India, and China.

1. The BRIC countries are emerging as growing sources of new technologies that may compete with products sold by many Western corporations, and
2. Corporations must analyze the massive consumer markets developing in BRIC countries.

These developing markets are changing the landscape concerning the relative importance of Western markets versus markets in developing countries.

**Ellen Richstone**  
**CFO, Sonus Networks; Director, American Power Conversion, Inc.**

The two risk areas that I think of most are:

**Monitoring Your International Operations.** As U.S. companies grow, international growth is a large part of market expansion. How much time is devoted to understanding what investments are being made, what the return to the company is, and what the impact is on long-term return to shareholders—and over what time period?

For example, moving some operations to a lower-cost environment can often reduce costs. But has the company considered both the business risks, as well as the operational risks—and appropriately thought about them? If the company is investing in a new market overseas: What is the cost of the investment? What is the return? And what are the controls that will be put into place to monitor the business activity?

**Technology Paradigm Shifts.** How does the board really understand what is happening in the company’s technology and in the marketplace? What signs should the board be watching for in order to provide input on the company’s strategy? If it is a technology company, ensure that the board and the company understand both the technology risks and any marketplace shifts that could impact the company’s long-term decisions.

**Dave Landsittel**  
**Chair of the Audit Committee, Molex**

Risk assessment is a pretty visible topic among boards these days. While risks relating to financial reporting/Section 404 are now required to be addressed, my experience is that boards and managements are increasingly sensitive to the importance of risk management on a broader enterprise basis—beyond those risks affecting financial reporting. Such risks relate to legal compliance issues; relationships with customers, vendors, and competitors; and risks triggered by potential external events—for example, severe economic downturns, political instability in less developed countries, and other potentially catastrophic events, such as terrorist attacks or outbreaks of infectious disease.

One area that is sometimes overlooked involves risks that would have a *disproportionate effect* on the company’s reputation—for example:

- A product failure affecting a small subsidiary that triggers a more widespread impact on consumer confidence and loyalty toward the entire company, or
- Inappropriate activity or legal violations by management representatives at subsidiary locations that could result in widespread visibility and embarrassment for the entire company. Another important risk area that is widely applicable and sometimes overlooked involves the possibility of unanticipated management and employee turnover (e.g. to competitors) and general management succession risk.

In my view, the board’s role primarily consists of ascertaining that management has an effective, formalized process for identifying risks; for monitoring significant internal and external changes that affect risks; for periodically prioritizing the impact of risks based upon their significance and likelihood; and for taking appropriate steps to address or mitigate the risks. The board should not only understand the process but also can enrich the process significantly by discussing the subject and providing management with its views.

Finally, boards should assess and assure that there is an alignment between risk assessment and the company’s strategic objectives. Sometimes the risk management process is designed in a manner that is inadvertently too one-sided. In this regard, board members should consider asking questions such as: Are we too risk-averse? How can we balance risk management with value creation? How much do new products push the risk envelope?