FTI JOURNAL
September 2013

In *Any* Event:

ERM Through Business Resilience

Michael Flaharty
Managing Director
Forensic & Litigation Consulting Segment
FTI Consulting

FTI CONSULTING

The hurricane is not the risk. The risk is that the hurricane will disrupt your business. There's not much you can do about the hurricane; there's a lot you can do to make sure your business can recover.

Executive Summary

Companies are steadily embracing enterprise risk management (ERM), and stakeholders increasingly require it. Yet few companies have developed a plan to respond to the full range of threats that could affect the critical assets. A business resilience plan can enable companies to create comprehensive strategies based on a thorough understanding of the assets at risk.

Blind Spots

ERM's hallmark is its intended comprehensiveness. It is an enterprise-wide approach that (ideally) accounts for the full range of risks that could affect an organization. But, in reality, most ERM plans don't.

The problem is that ERM tends to emphasize threats to particular classes of assets, most often related to finance, information technology (IT) and data, as well as to factories and equipment. This emphasis may cause companies to neglect other assets that are more difficult to measure or quantify such as human capital or third-party suppliers and partners.

Moreover, most companies start by establishing a plan to minimize the impact of particular threats before identifying all the critical assets. For example, a company may invest to protect a factory from the danger of flooding without ensuring that the power plant that supplies the electricity is protected from this risk. In such a case, the power plant is a critical asset the factory must have to operate, and a thorough risk plan must take this into account.

A business resilience approach calls for companies to identify the full range of their critical assets and then develop event-neutral strategies to prevent or minimize the effects of potential disruptions.

This enables organizations to frame more comprehensive and effective risk strategies. For instance, a company that has a strategy to get a warehouse up and running after a hurricane may seem to be well-prepared if a hurricane hits. However, the recovery requirement changes if the hurricane prevents suppliers from delivering materials or if it knocks out a supplier's network portal for processing orders. A good strategy needs to address the loss of the warehouse's functioning along the length of the supply chain, regardless of the cause. In other words, protection of a company's assets may need to extend beyond its physical boundaries.

The Risk of Neglected Assets

The tendency to emphasize certain types of assets and events leads companies to overlook possible critical assets whose disruption could severely damage or even bankrupt businesses.

Most companies keep a close eye on financial and productivity metrics. However, organizations may be less vigilant about risks related to cost cutting, especially in turbulent economic times. For example, a lean Fortune 500 retailer that increased productivity by drastically reducing headcount later was surprised to discover that there were only a few people left on staff capable of running the proprietary software. If any of the remaining staff members were lost, the company wouldn't be able to function. The asset at risk was process knowledge possessed by employees, some of whom had been dismissed, thus leaving the company with virtually no backup resources.

Indeed, few companies have sophisticated mechanisms for identifying the hidden risks that arise from the increasing interdependency of assets. For example, IT groups usually have detailed strategies for dealing with network disruptions, but these tactics often don't accommodate the recovery priorities of other divisions — such as finance, sales or distribution — whose processes depend on the network. Does IT know which business process is most important to finance, which system is most critical to its operations and how each should be prioritized as the network is rebooted?

Start with "What's at Risk?"

Business resilience is a philosophy and set of tools for ERM that focus on assets, not events. The approach is event neutral because it chiefly is concerned with how the disruption of an asset affects an organization, regardless of the cause of disruption.

Organizations must define "asset" as broadly as possible to gain a comprehensive view of the full range of risks that could affect a company. The concept should include everything from hard holdings such as factories and equipment to soft ones such as processes, relationships and reputation. Indeed, companies need not own something for it to be a critical asset; it may belong to another entity or the asset may be shared. An asset is anything that if disabled or unavailable, for whatever reason, could affect a company's ability to remain viable.

The first step along the path to resilience is to identify the full range of assets whose disruption could adversely affect an organization (see the following section on business impact analysis (BIA) for details about how this is done). This is a more achievable goal than identifying and managing every possible risk.

As part of this process, organizations also should evaluate their property and business-interruption insurance policies to determine the true breadth and depth of coverage. Tools we have developed to assess insurance policies routinely indicate that coverage is not as extensive as organizations think. Companies that identify important coverage gaps often can negotiate better terms with their insurers. Those companies that can't should address the gaps in the risk plans.

Once a company has a comprehensive view of its assets, it should prioritize them based on how much the organization would be affected if they were disrupted. Assets whose disruption will cause enterprise-wide effects in a short time frame must be ranked as top priorities. Lost or unavailable assets that are likely to cause only regional or local effects can be tagged as lower priorities.

Companies then should develop event-neutral strategies for mitigating the risk of disruption of the priority assets. The general plan eventually will be tested and refined based on event-specific scenarios — indeed, events do matter — but it is important not to prepare for particular events until a general plan has been established. Why? Because the general plan enables companies to address any disruption, regardless of its cause. If a factory is incapacitated, a general plan can enable the owner to recover from the disruption whether the cause is a natural disaster, a technological error, a labor issue, a breakdown in a supplier's operations or a terrorist attack.

The first step along the path to resilience is to identify the full range of those assets the disruption of which could adversely affect the organization.

No company can prepare for every eventuality — or even imagine every risk it might face. With event-neutral plans, companies are prepared for events that might never have been anticipated.

In the end, the only way to gauge how well a general plan works is to test it with event-specific scenarios. And companies should develop specific plans to deal with the particular risks posed by events that are highly likely to occur. Those companies with assets located near flood planes, for example, should have a specific flood plan.

These particular plans usually will be extensions of the general plan a company already has developed.

The Path to Resilience

Companies must have a comprehensive and detailed understanding of all their business processes in order to list the full range of risks that could affect the business. But surprisingly, most don't. The knowledge usually is dispersed throughout an organization; it is not consolidated in a way that would enable a company to have an overall view of its risks.

To develop a comprehensive view, companies should conduct an asset-focused BIA that will enable them to map how each business process works in detail, from beginning to end. This involves interviewing a broad cross section of internal stakeholders as possible, as well as surveying external suppliers and partners to identify assets that range from raw materials to relationships. These activities also will enable a company to evaluate its existing mechanisms for managing risk, as well as assess its tolerance for risk.

Questions should include: What are the activities the group undertakes? Who is involved? What inputs are required, and how are they sourced? What facilities and equipment are used? What other types of resources are required? What

are the outputs, and how are they delivered?

For each asset identified, interviewers also should ask what would happen to the business if the asset was not available. What if a supplier is unable to deliver a part? What if certain employees can't get to work, the network goes down or a line of credit is frozen? How long can the company remain in a diminished state before customers migrate to competitors? These discussions enable interviewers to determine whether a particular asset is critical, important or non-essential.

Interviews are best conducted by people outside a specific function. For example, an interviewer working with (but not employed by) a furniture manufacturer asked about a bin of connectors he noticed on a factory floor. He learned that 50 or more connectors are used in each piece of furniture but that the company kept a 10-day supply on hand and had only one supplier that delivered through the Port of New Orleans. The company stood to lose significant market share if the supply of connectors was delayed by 20 days. People inside the factory wouldn't have asked about the connectors; they were part of the landscape and effectively invisible. But because the interviewer was not familiar with connectors, he asked — and discovered an unrecognized critical asset with a significant associated risk. The company then reduced that risk by enlarging its pool of suppliers. It also persuaded its existing supplier to open a second delivery route through the less hurricane-afflicted Port of Long Beach.

Organizations that conduct thorough BIAs often are surprised by what they find. An academic institution that had a detailed plan for keeping its IT network running was surprised to learn that researchers and students had plugged hundreds of homegrown applications into its servers that posed serious risks to the network.

Unfortunately, many companies don't discover important external interdependencies until a disruption occurs. A credit union in New York accelerated payroll processing on the eve of Superstorm Sandy to ensure customers would receive their paychecks before the storm hit. But despite the company's efforts, an intermediary responsible for making the payments suffered a network outage, and checks weren't delivered for two weeks. The credit union thought it was effectively managing its event-related risk, but the organization didn't consider how it might be threatened by risk a provider faced.

Developing Event-Agnostic Plans

Once the business impacts are understood, companies can develop a plan that will help to avoid or mitigate disruptions of priority assets, regardless of the events that cause such disruptions. For example, a company that pinpoints a particular factory as a high-priority asset needs a plan that can be used to start the process of bringing the factory back online no matter what caused the disruption. The plan may involve framing a communications protocol that sets out clear guidelines about who to contact first in case of an incident and how to assemble the most important staff to begin problem solving. The plan might establish possible protocols for dealing with customers and financial institutions so the company can make arrangements for lapses in production. And the plan might identify partners to whom the company could turn for outsourcing parts instead of manufacturing them internally.

After a general plan for all priority assets is prepared, the company can begin to test that plan against event-specific scenarios. What if the plant was shut down because a flood destroyed critical equipment? Or what if a supplier was suddenly put out of commission? Or what if the IT network crashed in the wake of a cyber attack? The company should revise its plan based on how well these scenarios perform in response to simulated events.

Once a general plan has been laid out, a company can develop specific plans to address the risk of disruption from events that are very likely to occur. For example, a plant located near a fault line should have a strategy for dealing with possible disruptions caused by earthquakes.

True resilience can be achieved only by companies that have a comprehensive understanding of the full range of their real assets. This includes assets that may be difficult to measure (such as the organizational knowledge of employees approaching retirement) and assets that easily can be measured (such as real estate and equipment). The assessment should include assets the company owns, those that are shared, and those owned by suppliers and partners that are critical to the organization's functioning.

The most resilient companies are aware of and understand their most important business assets in the broadest possible sense and develop a general plan to manage risks to those assets regardless of the cause. By doing that work first, companies can establish event-specific strategies that make business sense.

Michael Flaharty
Managing Director
Forensic & Litigation Consulting Segment
FTI Consulting
michael.flaharty@fticonsulting.com

For more information and an online version of this article, visit ftijournal.com.