10 Things You Don't Know about Managing Your Business Operations Risks

By Neil Kaufman

Operational risks are those that impact the continuity of your core business functions. Whether the precipitating event is severe weather, a dock strike, an act of internal sabotage, a pandemic outbreak that takes out your supply chain, or an act of terrorism, the interruption of normal functions can have severe, long-term consequences. Left unaddressed even for a brief period, these interruptions can quickly lead to a loss of market share, erosion of a brand's reputation, noncompliance with regulatory mandates, and ultimately, even business failure.

Given the high stakes involved, we would expect that business owners, managers, and board members would place a high priority on devising practical and effective approaches to both recognizing and addressing their firm's operational risks. But shockingly, many organizations exhibit poor risk management, with a surprising absence of basic controls and oversight.

These companies believe that they have effective plans to ensure operational continuity after a disaster. But a closer look tells a far different story. Many have accomplished the corporate version of "checking the box" to comply with insurance or auditing regulations. But well-defined plans that have the backing of senior management and that have been exercised and updated regularly through simulations are the exception, not the rule.

The following are ten items that you may find surprising—from an insider's perspective—about the true state of your firm's operational risk exposure. If they sound familiar, have an expert or your insurance broker conduct an outside assessment. Their suggestions will help you sleep better at night.

1. **IT may not have it under control**. Your IT department's plan to restore technology infrastructure, recover network functions, and support your critical applications may not be sufficient. Due to the political and functional silos that exist in many organizations, systems recovery priorities are often not driven by business users, as they should be. In addition, human factor elements are often overlooked.

2. **Top management may not "get it."** The company Website may mention operational continuity and the annual report may brag about it, but many CEOs know that they really do not have a workable strategy in place and that the operations impact could be catastrophic. Without top management commitment to business continuity and a well-defined risk management function, it is doubtful your plan could withstand a real crisis.

3. **Do you have a strong emergency/crisis plan?** Business continuity deals with sustaining the core operational functions of the company. You can minimize the stress on the organization by establishing front-end emergency/crisis response plans that can prevent or minimize the impact of critical incidents occurring in the first place or can enable your company to respond to them and recover from them faster.

4. **Go local.** Your city or county health department has well-defined plans, policies, and procedures should an infectious disease pandemic occur, so integrate your emergency/crisis plan with this community plan. But it is the result of the public health emergency—you could lose 40% or more of your personnel for an extended period of time—that poses the real business continuity risk to the organization. You have to determine how your business could continue to function if almost half of the employees can't come to work.

5. **Assess your insurance situation.** Your risk management department (if your firm has one) understands how to buy traditional insurance coverage but may not understand the underlying operational risks for which it is buying insurance. So make sure your insurance broker and underwriter have a really good idea of your exposures so that you'll have adequate business interruption, contingent business interruption and extra expense coverage.

6. **Get your legal department involved.** Emergency plans exist to protect lives, property, and assets. Business continuity plans exist to ensure that the company can quickly resume normal operations in spite of catastrophes. But both can also play an enormous role in helping your legal department defend your company against lawsuits and reduce the size of any settlements. The best way to do this is to ensure that your plans meet regulations, standards and industry best practices. Anything less exposes your company to greater financial risk.

7. **Reevaluate alternate work locations.** IT "hot-sites" and pre-arranged temporary facilities may be located within an area that is impacted as negatively as your original location. Make sure that these secondary locations are on

a different power grid, are served by different network providers, or are located far enough away that impacted infrastructure does not restrict their practicality. Also, keep in mind that “hot-site” contracts are often “first come/first served.” Since you are not necessarily guaranteed space, be sure to plan accordingly.

8. **“Show me the paper.”** Effective operations continuity plans establish procedures for storing hard copy versions of vital records. We were told that the Internet age would render hard copies relics of the past. Instead, every Web page and every version of our documents seem worthy of printing…and storing. For many professions—law firms, for example—access to hard copies is critical. Don’t think you’re safe just because you’ve backed up your computer files.

9. **Business continuity simulations are *meant to fail*.** Make sure that senior leadership understands that there is no such thing as a passing grade when you are talking about organizational survival. If you passed the simulation, go back and do it again, because you missed something.

10. **Keep it current.** A strong annual maintenance process is the proverbial “ounce of prevention” in business continuity. Old plans gather dust and are ineffective unless they are “brushed off” regularly, tested, and updated to accommodate the changing dynamics of your business. Think of them as the company’s “last will and testament” that need to be revised from time to time to reflect new business realities. And, p.s.: make sure every employee has access to the latest version of the plan.

About the Author:

Neil H. Kaufman is a senior vice president and national business/governmental continuity management practice leader at Risk Solutions International LLC (www.rsi-llc.com). He has 19 years of consulting, operational, communications, and systems industry experience and is a Certified Business Continuity Professional.