

Risk Intelligence in the age of global uncertainty Prudent preparedness for myriad threats



Preface

In the first decade of the 21st century, several public health issues caught the attention of the world community, including SARS in 2003, avian flu in 2006, and swine flu in 2009. Despite the initial publicity, none of these cases developed into the full-blown pandemics that some people feared.

Yet these cases did have one significant impact: they reemphasized the need for the “prudent preparedness” cited in this document.

In this second edition, we have reexamined our recommendations and conclusions, refreshed some of the examples, and updated facts and figures.

We believe that the paper’s founding premise has withstood the test of time:

The event may be a global pandemic, or it may be something completely unanticipated. The specific occurrence matters less than the acknowledgement that bad things happen and prudent companies prepare for them.

Our recommendations, which begin on page 7, will help you with your preparations.

Preface to the first edition

This publication represents the second installment in our series on “Risk Intelligence.” The concepts and viewpoints herein build upon those discussed in the first whitepaper in the series, *The Risk Intelligent Enterprise: ERM Done Right*. That document may be obtained free of charge at www.deloitte.com/RiskIntelligence.

As explained in the prior paper, one of the most significant characteristics of the Risk Intelligent Enterprise™ is a “risk management philosophy that focuses not solely on risk avoidance, but also on risk-taking as a means to value creation.”

That point is important enough to reiterate, however briefly, in this paper. But readers will note that the topic at hand — preparing for a seemingly infinite variety of severely disruptive events — lends itself more to a focus on risk mitigation and avoidance, rather than on risk-taking for reward. The narrower focus of this paper shouldn’t obscure the bigger picture, nor does it represent a change of perspective on our part. As we state in the first title:

“Organizations that are most effective and efficient in managing risks to both existing assets and to future growth will, in the long run, outperform those that are less so. Simply put, companies make money by taking intelligent risks and lose money by failing to manage risk intelligently.”

Risk Intelligence in the age of global uncertainty

Prudent preparedness for myriad threats

Peruse the news and you may reach an inescapable conclusion: The world is an exceedingly dangerous place — and getting more so all the time.

Myriad risks — real and perceived — assault us from all quarters: terrorism and war, data privacy and IT security breaches, natural and manmade disasters, market instability and currency crises, hazardous waste and industrial accidents, overtaxed power grids and fuel shortages, and on and on.

How we as individuals deal with this deluge of worries is a private matter between ourselves and our deities, psychologists, and/or loved ones. But how we as business people perceive, address, and manage risk should not be left to fancy or fate. Quite simply: too much is at stake.

Global pandemics: A genuine threat?

With predictable regularity, media outlets across the globe report on the latest potential pandemic. The stakes are high: According to the U.S. Department of Health and Human Services, “A worldwide influenza pandemic could have a major effect on the global economy, including travel, trade, tourism, food, consumption and eventually, investment and financial markets.¹”

While such pronouncements are sobering, here’s a contrarian thought:

Dire warnings about global pandemics are irrelevant.

Not to say that the specter of virulent disease isn’t of great concern. But in terms of your business, it doesn’t really matter whether these grim predictions come to pass, because if this pandemic doesn’t get you, almost assuredly, something else will. History tells us that over the next few years and decades, major disruptive events of all sorts *will* occur, and businesses caught unprepared *will* suffer. In the age of global uncertainty, the only surety is that bad things will happen to good companies.

Consider, for example, the effect on your business if worldwide oil deliveries were drastically curtailed due to

war, terrorism, or natural disaster. (This example is not as remote as it seems, bearing in mind that the U.S. keeps only about a 62-day supply in the Strategic Petroleum Reserve².) Or imagine a lengthy labor stoppage halting oversea shipments of key inventory components. Envision a computer virus that wipes out your company’s servers or telecommunications for an extended period.

Fortunately, companies that understand and prepare for the inevitability of business disruption will emerge in better shape than those that adopt a head-in-the-sand approach. A pandemic may or may not materialize, but it does provide Risk Intelligent organizations with a motivation and an opportunity to deal with the issues that arise from fundamental and substantial business disruption.

Beyond providing a rationale to act, predictions of a pandemic also offer an opportunity to broaden one’s thinking about risk. In an interdependent world, a myopic approach no longer suffices. Today, the potential impact of a business disruption extends well past your own walls, reaching upstream to your supply chain and downstream to your customers. Your business partners’ threats are your threats, and vice versa.

Additionally, companies need to think beyond traditional business continuity planning. It is no longer enough to ask, “Do I have an offsite place to store data?” or, “Can I shift production to another facility?” Now, companies must also consider what happens if many sites are rendered inoperable or if people can’t show up to work for an extended period of time because of illness, edict, or energy crisis.

Companies that take steps to improve their shock resilience *before* an event takes place will clearly have an easier and faster recovery, as well as competitive advantage in the marketplace. Even more importantly, the resilience of the businesses that form our critical infrastructure — financial, energy, utility, construction, and other companies — not only benefits the company, but also immeasurably serves the public interest.

¹ “Economic Impacts,” U.S. Department of Health and Human Services, <http://www.pandemicflu.gov/impacts/index.html> (accessed 13 May 2009).

² <http://www.fe.doe.gov/programs/reserves/spr/spr-facts.html> (accessed 13 May 2009).

Sudden impact

In our first whitepaper in this series, *The Risk Intelligent Enterprise: ERM Done Right*, we recommended that companies engage in scenario planning to augment statistical modeling and help prepare for specific events. Scenario planning enables executives to answer the questions: “What could disrupt our plans? And how vulnerable are we?”

This process is valuable, but once companies have integrated scenario planning into their risk management protocol, it is time to initiate a complementary practice: business impact analysis. This process fills a critical knowledge gap, because while the prospect of disruption may be almost certain, the causes are often unpredictable.

A business impact analysis can help illuminate the ways that your company could be affected, regardless of the cause, and can identify the major impacts, including financial, human, legal, stakeholder, reputational, health and safety, and environmental, that could result from an event or series of events.

Ask yourself: What is my company’s resilience in relation to:

- a major credit downgrade?
- stakeholders boycotting our products?
- the loss of key facilities for an extended period?
- an intense reputational crisis?

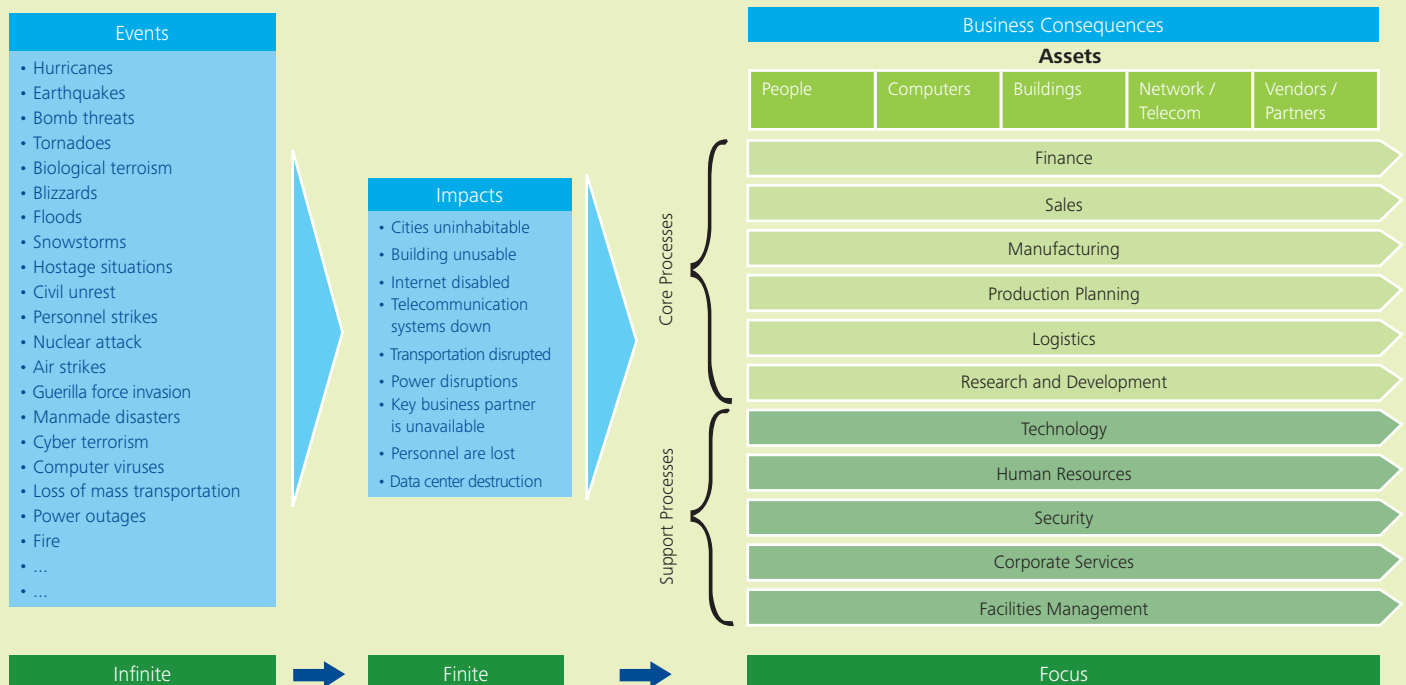
The possible negative scenarios are virtually limitless. The business impact analysis addresses this problem: there are simply too many variables to foresee every adverse event — or series of events — that your company may have to deal with.

What are some possible impacts? We’ll briefly address three:

People: One distinguishing characteristic of a pandemic is the disproportionate impact on people. Many other types of business disruptions, such as terrorism and hurricanes, include significant loss of property and infrastructure. Pandemics (naturally occurring or bio-terror), on the

Business impact analysis

An infinite set of events may impact your business in a finite number of ways. Avoid the mind-numbing analysis of potential events and focus instead on their impacts and business consequences.



other hand, primarily affect human capital. For example, in a crisis, companies may experience a high level of absenteeism throughout the organization, from senior management to operating staff. People may be unable or unwilling to report to work, staying home not just because they themselves are sick, but perhaps out of fear, to care for other ill family members, due to government decree, or because of transportation issues. Risk Intelligent companies will establish contingency plans to enable work to be performed remotely to maintain business continuity during extended worker absences.

Supply chain: Your company's supply chain may also be vulnerable. Various disruptions can make raw materials difficult to procure; the negative effects could ripple through production, inventory, and distribution. Heavy interdependencies with suppliers and sources demand vigilance in structuring and monitoring these relationships. Indeed, if you don't mandate this for your most important suppliers, all the advance planning within your organization may go for naught, given the inevitable shortages.

Companies might also reconsider reliance on sole-source suppliers. Although these relationships were originally intended to reduce costs, in today's environment they can lead to "concentration risk" and potential vulnerability or disruption.

The unfortunate reality is that supply chains can be weak links, and strong companies can be undermined by poorly prepared partners.

Finances: The financial impact of a disruptive event is sometimes overlooked. If your customers' financial systems are down and they can't pay you in a timely manner, could your company survive the cash flow crunch? If transportation and distribution systems fail and you can't get your product to market, how will that affect your ability to meet your financial obligations? In making contingency plans, you should consider such items as committed lines of credit and capital reserves, as well as your company's ability to rapidly implement tactical cost reductions and workforce reassignment as the need arises.

Prudent and practical preparedness

Of course, many variables come into play as you assess possible impacts, including industry, geography, size, structure, and other factors. But in all cases, the situation calls for constant vigilance and prudent and practical preparedness.

As your company assesses the wide range of possible events and business impacts, you should also consider the continuum of preparedness — the least to the most that you can do to prepare.

Of course, you can't prepare for everything. Thus, the challenge becomes to determine what's practical and prudent. How can you get the biggest bang for the buck? How can you cover the widest range of business impacts for the broadest range of events? How can you protect your ability to conduct business?

The Lessons of Katrina

Hurricane Katrina devastated New Orleans and surrounding areas in 2005. For all the misery it brought, Katrina also provided a number of excellent risk preparedness practices. For example, availability of power is a prerequisite for most companies to get back up and running. Knowing this, a major retailer outfitted the back of each store with a high-capacity electrical outlet, allowing them to simply back up a portable generator and plug it in. A national healthcare provider moved medical supplies to the perimeter of the hurricane strike zone. A large beverage company stopped bottling beer and started bottling water.

Again, each situation is unique, and what makes sense for one company may be inappropriate for another. Each organization should make a conscious, informed decision as to what level of risk to accept. At the end of day, executives and directors must be able to say — to boards and other stakeholders (customers, regulators, shareholders, analysts, communities, employees, etc.) — that they have done everything reasonably within their power to prepare and respond to business disruption.

Executives should ask: What risks can we reasonably prevent, detect, and respond to?

In many instances, the most effective (but not always the most viable) choice is prevention. The Year 2000 computer problem provides an example: Countless dollars and worker-hours were devoted to correcting the programming glitch that threatened to leave many computers unable to read 21st century dates. And the massive project appears to have been a success: very few of the anticipated computer malfunctions materialized. Yet at the same time, the very lack of problems as the century turned led many people to believe that the effort was a waste of time and money. Unfortunately, it is difficult to prove you prevented something that never occurred.

If an event is beyond your control or ability to prevent, then detection, response, and recovery come into play. Detection, of course, requires systems in place to provide sufficient warning to allow for a response. The earlier the detection, the greater your ability to intervene successfully, whether reacting to a physical burglary or a breach of cyber security. See the appendix of this document for practical steps you can take in these areas.

Planning doesn't necessarily entail spending considerable sums of money; many activities can be conducted at little or no cost. For example, significant advantage can be gained by having response teams identified in advance, along with predetermined responsibilities and authority. Conduct team meetings where employees discuss potential actions to take in a disaster. Address fundamental steps that sometimes get overlooked, such as who declares when a disaster has occurred and who initiates the company's emergency plans.

Speed of onset

Among the many arguments for vigilant preparedness is the "speed of onset" factor. While certain risk scenarios may play out with advance warning, others may arrive unannounced and with overwhelming speed. In such instances, well-formulated plans may represent the difference between fast and slow recovery.

In the case of Y2K, onset was slow. The vulnerability was known years in advance and the potential impact was well-documented. Nobody was taken by surprise at 12:00:01 a.m. on January 1, 2000.

But other disruptive events do not telegraph their arrival. A breach of cyber-security, for example, hits without warning; usually the event is not detected until the damage is done.

Thus, a corollary of speed of onset is speed of response. Some companies may find that even though they have established — and perhaps even tested — response plans, in the stress of the moment they may have difficulty implementing the plan as quickly as conditions require. The ability to move swiftly as "real-world" events unfold should be factored into the planning and testing process.

Although publicity around potential pandemics often borders on hype, it does serve one important purpose: awareness levels are high and no one can say they weren't warned. Risk Intelligent executives will take advantage of the lead time provided them to reevaluate their preparedness.

Recommendations

Once the threat of a potential pandemic is properly placed in the larger context, the question of "What now?" becomes predominant. How can companies begin to take control of the issues around severe business disruption?

A good place to start is with our Risk Intelligence whitepaper series. A wealth of titles, covering various industries, business issues, and occupational concerns, has been published. Each contains a listing of initial steps to bring Risk Intelligence to your organization. (Visit www.deloitte.com/riskintelligence to order or download copies at no charge.)

Here are some additional items to think about and activities to engage in.

Build a business case: In the not-too-distant past, risk management was often given token attention. Many times a risk assessment would be conducted, but then the recommendations would sit upon a shelf.

Today, of course, an assessment can no longer be a token exercise: follow-up action is paramount. Heightened awareness around risk issues means that executives and others responsible for coordinated risk management can make a more compelling case than ever before. Attention can be drawn to the relative costs of poor versus good risk management. The point can be convincingly made that improved shock resilience will provide competitive advantage. And, in this age of emphasis on good corporate citizenship, a culminating argument can be presented: Having a viable Risk Intelligence plan in place to deal with various contingencies represents a socially responsible choice.

Assess risk: Using techniques such as scenario planning, business impact analysis, vulnerability assessments, statistical modeling, and other methods, companies should assess their risk exposure. Some questions to be addressed:

- What could a disruptive event look like?
- What are the potential business impacts?
- What are the competitive impacts?
- What are the upstream and downstream impacts on the company's or industry's value chain?
- What is the level of readiness and resilience of the company, as well as its suppliers, distributors, and customers?

Consider the people impact: As noted above, pandemic and bio-terror threats may exert a more significant impact on the work *force* than the work *place*. As such, it is important to have the right infrastructure and processes in place so that people can work remotely if the need arises. Many companies are improving their capability to have employees telecommute. This may involve equipping employees with laptops, cellphones, and other mobile devices (with replaceable — not rechargeable — batteries); it can include providing broadband or dial-up connectivity; installing a VPN (virtual private network) to enable secure, remote access to the company's servers; and it should include load-testing the capacity of the system to ensure that it can handle a sudden influx of users.

Of course, preparedness is not solely about laptops and Internet access. Consideration must also be given to management processes, because companies need to attain the same consistency in key activities wherever they are performed. Attention should also be paid to training and performance metrics. The goal is for the business to run as well as before the migration to telecommuting took place.

Yet not every business lends itself to remote work. If employees require access to large machinery or equipment, or to clean rooms, dry rooms, or other specialized environments, different strategies must be employed. In a pandemic situation, possibilities include running multiple shifts or employing social distancing techniques to minimize face-to-face contact. Companies could also closely track employee health and try to utilize workers who have recovered from the disease and may have developed immunity to it.

Think expansively: Some threats may impact a geographic area that is significantly wider than a single plant or facility. In such cases, a commonly employed strategy — “If this plant has a disruption, we'll move operations to another site” — may not be viable.

Preparedness for certain categories of severe business disruption should not be limited to single location, but should include all mission-critical sites, irrespective of geography.

Look outside your walls: For many companies, an even wider net should be cast, one that captures both upstream and downstream entities, i.e., supply chain partners, distributors, customers, lenders, and other counterparties.

The interconnectedness and interdependencies of today's business world means that your due diligence around risk management must extend beyond your company walls. Any vulnerability in the supply chain or distribution channels could lead to a “weak link” scenario that could grind business to a halt. As such, it is important to hold your suppliers and distributors to the same standards as you hold yourself.

Verbal assurances from your partners should not suffice. A more-prudent course will require verifiable evidence of business continuity and disaster recovery plans (and the testing of those plans) from all significant business partners.

Also, overdependence on a limited number of suppliers should be weaned, if possible. Companies may wish to take steps to expand their supply chain before a disruption takes place, rather than scrambling to do so after the fact.

Evaluate outsourcing arrangements: Many companies depend heavily on third-party providers to deliver critical services, and, until recently, there have been many compelling reasons to do so. However, just as a weak supply chain link can undermine preparedness, so too can extensive use of outsourced providers. The same approach applies: Carefully scrutinize these relationships to make sure your providers have in place robust disaster preparation and recovery plans.

Conclusion: Making the Risk Intelligent choice

History provides strong evidence that a significant disruptive event is an inevitability, not merely a possibility. If you accept that premise, then inaction becomes an exceedingly poor — even unacceptable — choice.

The event may be a global pandemic, or it may be something completely unanticipated. The specific occurrence matters less than the acknowledgement that bad things happen and prudent companies prepare for them.

The responsibility to anticipate, prepare for, and respond to a crisis may be shared among many, including businesses, governments, nonprofits, and individuals. Yet, in the end, it may be the corporate sector that must lead the recovery. History has shown that the government may not have the resources or the ability to take full control during highly

disruptive events. Citizens will look to businesses to help ensure that basic services are provided, and they will expect companies to work assiduously to get life back to “normal” as soon as possible.

Companies may also have an opportunity to expand or adapt their business to respond to a crisis. If proper planning and preparations are made, companies could help governments, communities, and other vital industries by providing expertise, goods and services, and/or volunteers. This “socially responsible” aspect of planning and response can greatly enhance a company’s image, while it may also provide new revenue streams for businesses highly susceptible to certain crises. To the extent a business can respond quickly to a crisis and assist in the recovery, a company can have a significant positive impact that reaches, but also transcends, the bottom line.

Appendix: Next steps

The fact that risk lurks around virtually every corner gives rise to corollary threats: executives and boards can be overwhelmed into paralysis; or they can deem the problem too large to ever be effectively managed, and thus choose to ignore it.

Yet while it's true that you can't anticipate or prepare for every conceivable risk, you *can* take methodical steps to separate the credible and realistic risks from the fanciful. And in the process you can create a strong case to justify the commitment of resources in the places that matter most. Investors, analysts, rating services, and even judges and juries, will be more inclined to look favorably upon a company that took steps to mitigate its risk exposure, rather than those that considered the problem unmanageable.

Of course, many companies have existing risk management structures and programs in place, with varying levels of sophistication. The discussion above and the steps below are not intended to supplant or invalidate work already done. Rather, they represent considerations to be weighed and selectively incorporated into existing programs, be they fledgling or well-established.

Activities can be broken into three stages: (1) anticipation and preparation, (2) first response, and (3) recovery. Here are some steps to consider for each phase:

Anticipation and preparation

The observation may be obvious, but given the lack of preparation at many companies, it bears repeating: Work that you do in advance of a disruption will serve you far better than trying to improvise in the heat of a crisis.

- Designate an individual to lead the Risk Intelligence planning effort.
- Appoint a Risk Intelligence steering committee.
- Determine your risk appetite; identify maximum allowable outages.
- Plan for the impact on your business. Identify critical assets: people, processes, systems, facilities, and intellectual property; determine the maximum allowable time you can go without them; factor these timeframes into your planning.

- Establish policies to be implemented during disruption.
- Establish procedures to back up the policies.
- Clearly define roles and responsibilities.
- Communicate plans with employees in advance of any event; ensure that you have adequately trained your people.
- Establish telecommuting guidelines and identify those who can and cannot participate in a telecommuting program.
- Recognize that senior executives required for strategic decisions may be incapacitated. Implement a plan of succession.
- Invest in capable people, processes, and systems.
- Establish emergency communication protocols and information pathways. (This is a critical area, as communications during crises is often extremely difficult.)
- Determine critical businesses; establish plans to redeploy personnel from other businesses to critical businesses.
- Determine critical functions; establish plans to redeploy personnel from other functions to critical functions.
- Consider key customers to serve at normal levels; i.e., evaluate whether you should allocate a disproportionate share of your available resources to your most important customers.
- Request risk management plans from partners and suppliers.
- Stress test your entire plan, using desktop exercises and real drills. Ensure the plan can be deployed as quickly and effectively as required in a real situation.

First response

The primary objective of the First Response stage is containing the problem — protecting people and facilities, the community, critical infrastructure, etc.

- Allocate resources to protect employees during initial disruption.
- Initiate emergency communication plan with employees.
- Determine employee location, condition, and situation.
- Communicate and coordinate with external partners.
- Coordinate with external organizations and help communities.
- Systematically monitor critical external events through media and other available means.

- Implement plans to deal with service shortfalls.
- Initiate plans to serve priority customers and clients.
- Monitor your systems and establish triggers to generate responses.

Recovery

The Recovery phase concerns business resumption — getting back to “business as usual” as quickly as possible. Short- and long-term activities compose this stage: the immediate recovery activities and the post-recovery reevaluation and adjustment.

- Continue to communicate critical and timely information to employees and key stakeholders. Don’t let the media be your only voice.
- Consider staggered or partial facility reopenings.
- Implement plans to resume mission-critical activities first.
- Communicate and coordinate with external parties regarding critical infrastructure needs.
- Work with local, regional, and national media to publicize best practices and success stories.
- Conduct a timely post-event review to identify weak areas and initiate improvements for future disruptions.

Contacts

Mark Layton

Global Leader, Governance and Risk Management
Deloitte & Touche LLP
mlayton@deloitte.com
+1 214 840 7979

Henry Ristuccia

U.S. Leader, Governance and Risk Management
Deloitte & Touche LLP
hristuccia@deloitte.com
+1 212 436 4244

Michael C. Evangelides

Principal, Pandemic Preparedness Consulting
Deloitte Consulting LLP
mevangelides@deloitte.com
+1 312 486 2739

Paul H. Keckley

Executive Director
Deloitte Center for Health Solutions
Deloitte LLP
pkeckley@deloitte.com
+1 202 220 2150

David Sarabacha

National Practice Leader, Business Continuity Management
Deloitte & Touche LLP
dsarabacha@deloitte.com
+1 206 716 7934

This publication contains general information only and is based on the experiences and research of Deloitte practitioners. Deloitte is not, by means of this publication, rendering business, financial, investment, or other professional advice or services. This publication is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your business. Before making any decision or taking any action that may affect your business, you should consult a qualified professional advisor. Deloitte, its affiliates, and related entities shall not be responsible for any loss sustained by any person who relies on this publication.