IDC
Analyze the Future

Global Headquarters: 5 Speen Street Framingham, MA 01701 USA P.508.872.8200 F.508.935.4015 www.idc.com

WHITE PAPER

Business Operations Disruption Risk: Identify, Measure, Reduce

Sponsored by: HP

Raymond Boggs
Jean S. Bozman
Randy Perry

December 2009

EXECUTIVE SUMMARY

Like the proverbial frog that never knows it's in danger as the cooking pot slowly heats to a boil, many of today's midsize organizations are not paying attention to the increasing temperature of their risk profile. As midsize companies continue to automate business processes, the information and communications infrastructure of successful midsize companies has gradually assumed greater and greater importance as a source of intelligence for senior management and critical information for and about customers. This computer-enabled infrastructure supports everything from order taking to providing products or services — and delivering those products and services to customers. Increasingly, a company's systems, data, and networks act as the heartbeat of the organization. Yet, how well do managers understand, measure, and mitigate risk in the event that this essential heartbeat falters or fails?

The loss of time, money, customers, and efficiency that system downtime[1] causes is damaging, but few midsize companies can measure downtime or calculate the impact of downtime on key aspects of their business operations. With all of the pressures midsize companies face every day, they typically lack the time and resources needed to understand the extent and nature of potential risk and how it might be reduced.

IDC studies across hundreds of midsize companies indicate a wide variance of failure rates and operating income loss as a result of system failure. Those at risk need to know it, measure it, and mitigate it. A growing number of midsize firms are looking carefully at their operations to find new efficiencies, apply new technologies, and implement new approaches to sharpen their business practices. Part of this updating of company processes and procedures involves identifying where vulnerabilities reside.

[1] In this white paper, "downtime" refers to *unplanned* downtime.

Adoption of Best Practices Reduces Downtime

But there is good news, as well, for those companies that plan to address business risk: The application of best practices across a company can reduce unplanned downtime by up to 85%.

Consider the impact of best practices, confirmed by interviews with multiple midsize companies:

- Consistent use of management software reduces network and system downtime by 65%.
- Upgrading servers/storage/network equipment reduces downtime by 50%.
- Enabling high-availability failover clustering software reduces downtime by 43%.
- Adopting industry best practices standards (e.g., ITIL, CobiT) across the organization reduces downtime by 13–15%.
- Using virtualization software, which isolates workloads and prevents interference between them, reduces server downtime by 10%.

This performance improvement/risk avoidance opportunity sets the stage for our discussion. For those organizations that need to increase their understanding of both the business risk and the risk management tactics of system downtime, this paper examines six key issues:

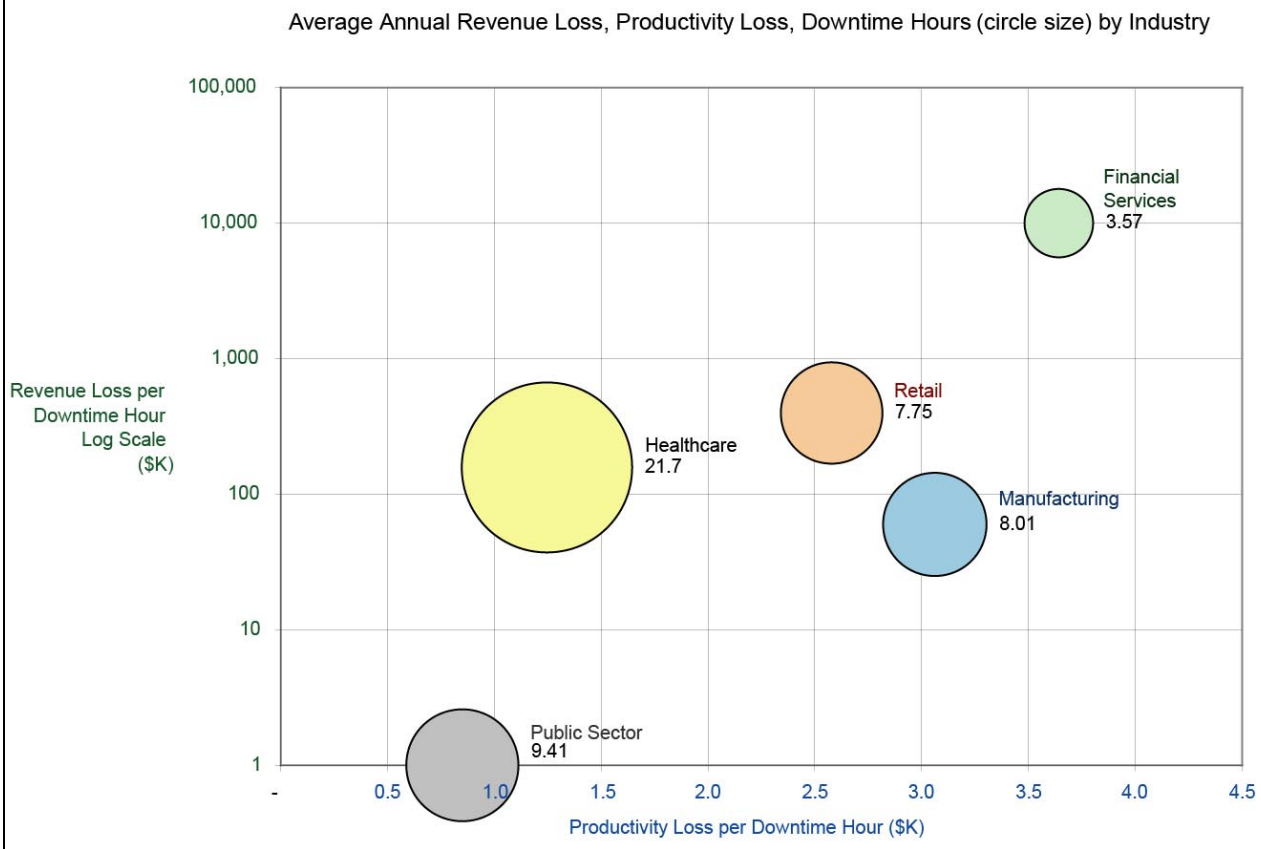
- Identification of business risk
- Variation in exposure to business risk
- Costs related to business risk
- Application of best practices to IT infrastructure
- Reduction of business risk and downtime
- Management of business risk on an ongoing basis

Business Risk: What Are We Counting?

The amount of business risk to which your company is exposed — and the impact of that risk on your business and on its revenue and profitability — will vary by company size, by vertical market, and by the types of workloads that go offline during downtime. Figure 1 shows the results of IDC research across industries — which clearly show the variation in downtime by industry and the dollar impact of periods of downtime on each of those industries.

FIGURE 1

Risk Realized: Revenue Loss, Productivity Loss, and Downtime Hours per Year by Industry



	Productivity Loss / Hour	Revenue Loss / Hour	Downtime Hours
Financial	$3.64	$9,997.50	3.57
Retail	$2.58	$397.50	7.75
Healthcare	$1.25	$157.50	21.70
Manufacturing	$3.06	$59.93	8.01
Public Sector	$0.85	$ .00	9.41

Source: IDC's Business Value Research, 2009

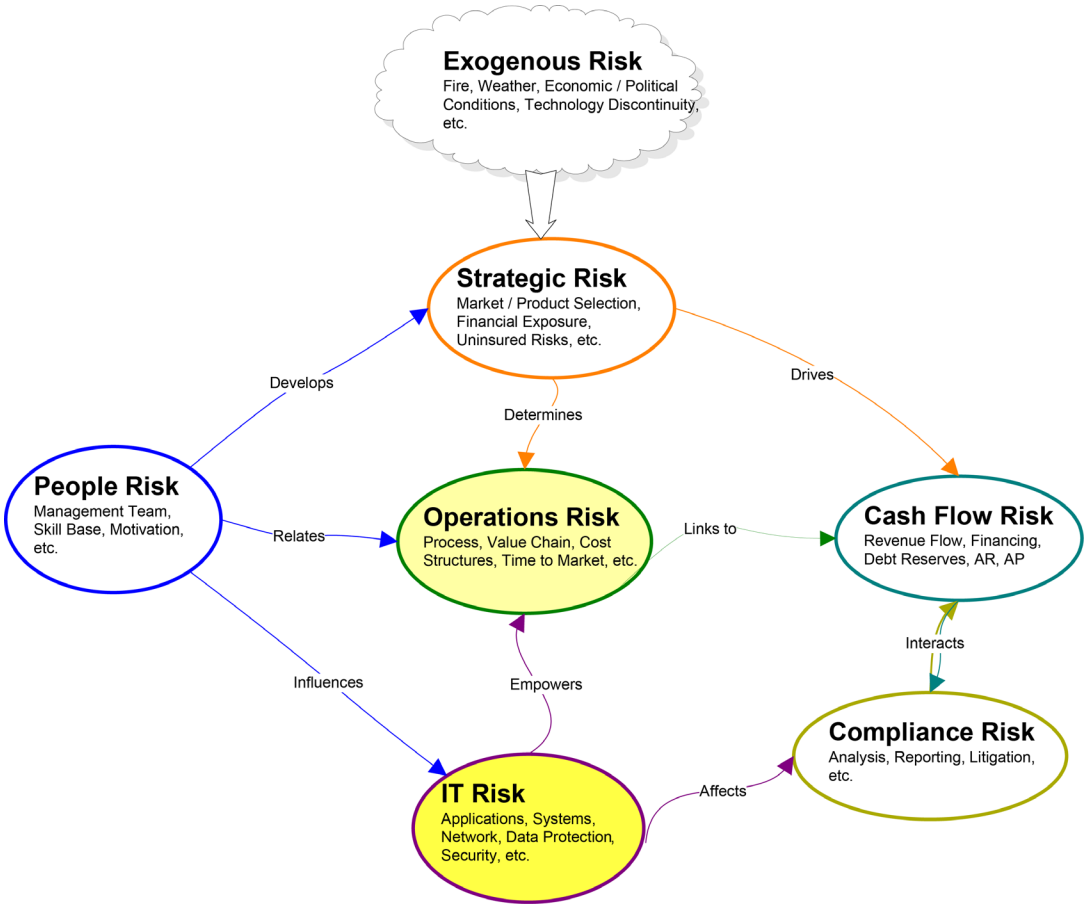
Industry by industry, the business view on business risk takes on a different flavor. For example, insurance and financial services firms define business or "enterprise" risk as the potential harm that may arise from some present process or future event. Professional risk assessments combine the probability of a negative event occurring with the amount of harm the event can cause. But even if the probability of an event is low (a car accident), the costs of the event can be high enough to justify advance preparation (buckling a seat belt).

Identifying Business Risk: An Example

For purposes of this discussion, we focus on a particular type of risk for deeper evaluation and planning. As Figure 2 indicates, business risks range far and wide and interact with each other.

FIGURE 2

Business Risk Types and Interactions



Source: IDC, 2009

While external or exogenous risks fall beyond management's control (and into the domain of insurance), much of business success depends on management's ability to effectively manage or reduce risks, such as:

- **People risk.** This risk category refers to the management and execution team's skills and ability, which will naturally change as a company grows.
- **Strategic risk.** This risk category refers to a firm's overall selection of target markets, investment in products and solutions, timing, financing, etc. In essence, strategic risk is the "vision risk" associated with long-term aspirations and how appropriate they are.

- **Operations risk.** This risk category is associated with how well a firm executes its core processes such as value chain management, customer relations, service delivery, etc. Midsize firms often focus on this risk category because of its apparent importance, but in reality, the dangers associated with operations risk usually reveal themselves quickly, allowing time for remedial action.
- **Cash flow risk.** Continuing financial viability depends on steady revenue flow, cost controls, effective accounting, billing success, and financing. While cash flow risk is easy to identify, the changing economic environment has brought new focus on this category.
- **Compliance risk.** Today, firms — especially publicly held firms — must comply with all required accounting and reporting standards. Compliance can also come from customer or supplier requirements, making the risk more financial (not winning or maintaining business) than legal (going to jail).
- **IT risk.** This risk category, which is our target, addresses the probability that applications, systems, networks, and data essential to business operations will fail.

  Our focus area (in Figure 2, see the shaded oval for IT risk and the more lightly shaded oval for the operations risk that it supports) is becoming a particular concern and target of enterprise risk management teams because so much depends on IT continuity. Although IT risk is only one part of a wider network of business risks that interoperate, it represents the type of risk that slips under the radar in many organizations even though it can have implications, near term and long term, for a number of other risk categories.

Downtime and Business Risk: How They're Related

The most important and critical dimension of IT risk relates to the reliability and continuity of the infrastructure itself — and the "dial tone" resilience of the infrastructure.

Using standard risk terminology, we define this aspect of IT risk as the probability of events or circumstances that lead to the disruption of operations and the consequent negative impact on operating income; that is, the likelihood that some combination of system or network failure, PC failure, or application or OS failure will prevent employees from doing their jobs or customers from being served.

Of course, downtime within one domain of the organization may or may not affect operations in another. For example, the failure of a factory-based computer system will not affect computer systems used for accounting or billing. However, many modern applications are, in fact, end-to-end applications, which touch many computers throughout the network. This means that disruption on one set of servers may ultimately lead to downtime in other servers that also support part of the end-to-end application.

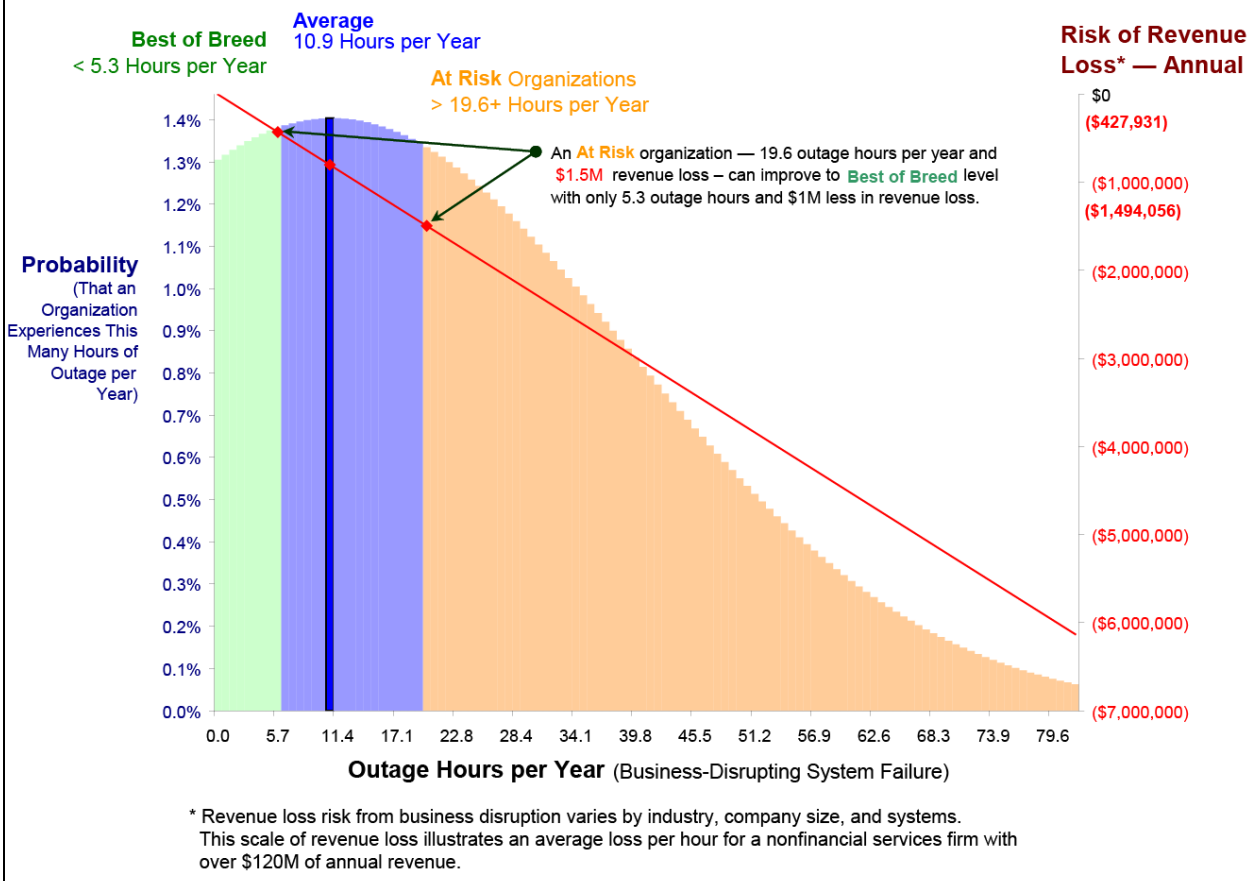
Now, let's look at the "big picture" — taking an organizational view. IDC measured this "down time" with 81 enterprises of various sizes and industries. We found that downtime affects different organizations in different ways, showing a wide range of values and exhibiting an even wider range of factors that impact the frequency of downtime. For midsize firms that have built their infrastructures over time, without considering the redundancy and resilience that might guide a newer approach, this

crossover vulnerability can easily be underestimated. Likewise, operating income loss risk from the business disruption caused by downtime varies significantly by industry, company size, and systems. The fact that it can be hard to measure ahead of time makes the impact of potential disruption no less harmful.

With these caveats understood, Figure 3 presents an overall view of the 81 enterprises and their relative experience with downtime.

FIGURE 3

IT Risk Scalar: Surveyed Organizations' Relative Experience of Business-Disrupting Outages and Resulting Revenue Loss



* Revenue loss risk from business disruption varies by industry, company size, and systems. This scale of revenue loss illustrates an average loss per hour for a nonfinancial services firm with over $120M of annual revenue.

Source: IDC's Business Value Research, 2009

The x-axis in Figure 3 lists the outage hours[2] per year experienced in a given organization — a measure of IT risk. This value ranges from a minimal zero to over 80 hours.

[2]IDC's "outage hours" refers to system downtime that causes business disruption during hours of business operation — typically 10 prime business hours per business day and 6 business days per week exclusive of holidays.

- The "average" organization experienced 10.9 hours of outage per year.
- "Best of breed" organizations (the 25% of surveyed organizations with the lowest failure rates) experienced less than half the outage hours of the average organization at 5.3 hours per year probability of failure or better.
- "At risk" organizations (which represented enterprises with the highest failure rates) experienced 19.6 outage hours or more per year. The exposure to outage among these organizations varied widely, from 19.6 outage hours per year to 80 or more outage hours per year.

The Linkage Between Downtime and Business Loss

System downtime can result in disrupted business processes, lower productivity, and reduced cycle times and activity rates. It also can cause employees to become frustrated with their inability to access key applications and data. But employees are not the only ones affected by downtime; unfortunately, in today's Web-enabled businesses, customers are, too.

During periods of downtime, organizations can lose customers who decide to go to other vendors or providers. The resulting diminished market reputation can also lead to reduced business from customers who remain. In short, over time, downtime and system-related issues can hurt profits as a result of both higher operating expense and lower revenue.

While loss from downtime ranges by industry type, company size, and relative reliance on systems, a consistent loss profile appears. The right-hand axis of Figure 3 shows the profile of revenue loss from downtime that a nonfinancial services firm with approximately $120 million in annual revenue would experience. As depicted, the risk of system downtime ranges from a level of 0.19%, or less, for a "best of breed" firm to a level of 0.66%, or more, for an "at risk" firm. This risk difference of a half a percent probability in downtime actually translates to over $1 million in increased risk exposure for the at-risk firm.

This IDC research data indicates that system downtime represents real business risk with hard dollar impact on a firm's bottom line. It shows that the risk of downtime varies widely by firm. As we discuss later in this paper, certain key risk components factor into this variation in risk.

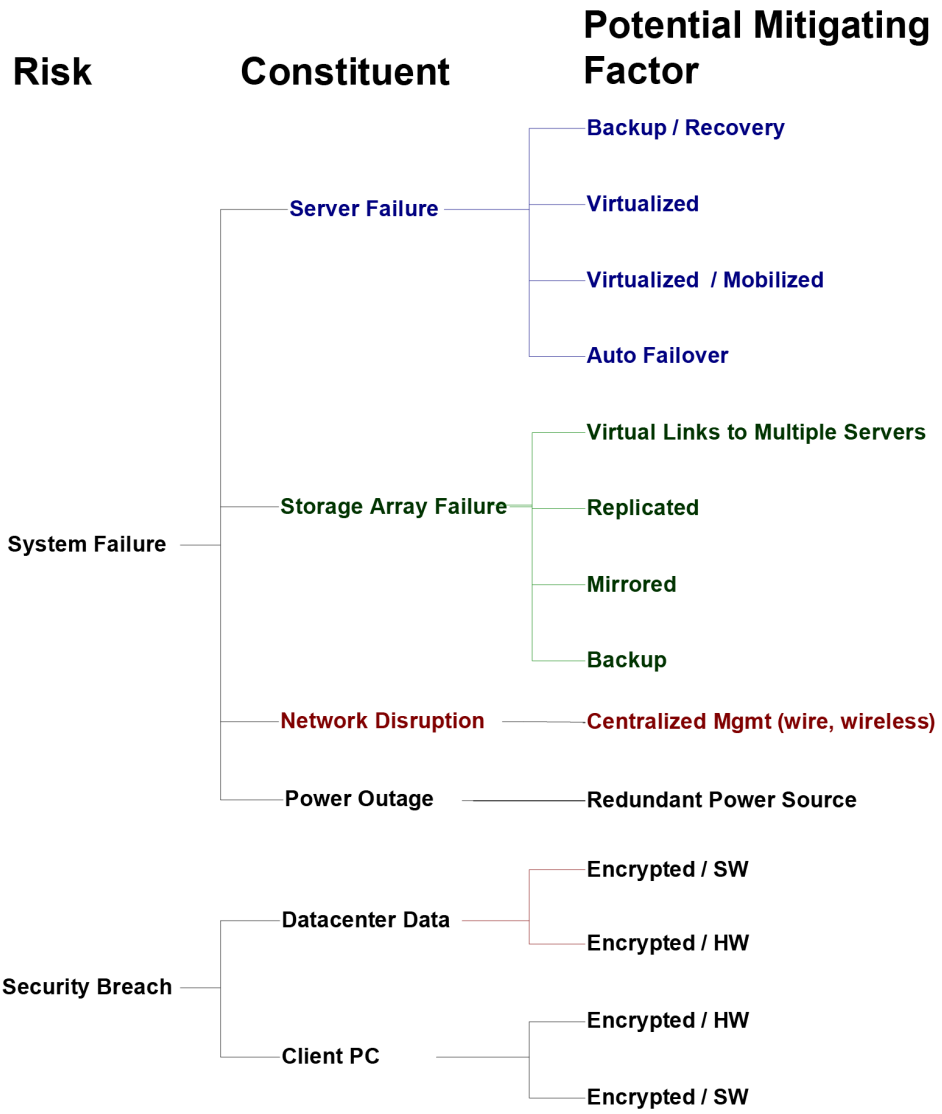
Looking Up the Causal Curve to Address Business Risk in IT

Effective risk management goes beyond identifying and measuring risk such as downtime to develop an understanding of the components and activities that contribute to potential failure. Understanding the multivariate nature of what may seem a single point of failure can help enhance protection or provide for more effective response plans.

As illustrated in Figure 4, system failures and security breaches can result from different subsystem failures. As can be seen, the presence or absence of different factors can influence the rate of failure — which in turn affects the business results. This type of analysis results in a more comprehensive view of risk — and the way in which it develops, over time, based on underlying causes. The more comprehensive a map of contributing factors you can develop, the more effective you will be at disaggregating the different vulnerabilities you have so that each can be addressed effectively in turn. Ultimately, the goal will be to improve the reliability (or recoverability) of the essential elements of your technology portfolio.

FIGURE 4

Risk Analysis and Mitigating Factors



Source: IDC, 2009

Action Plan for Business Risk Mitigation Evaluation

No one could expect a business to completely refresh its infrastructure — replacing all servers or updating all software — across the board. That would simply be too expensive, too time-consuming, and too disruptive to the practices in place at midsize firms. Instead, organizations should identify those aspects of their IT infrastructure that would benefit most from changes, updates, or repair — and address those issues first. Over time, other technologies could be changed, or replaced, while others will remain over a longer period of time. The process of identifying the importance of different parts of a firm's IT environment, along with their vulnerabilities, can actually reveal important opportunities for upgrades, especially if a comprehensive infrastructure review has not been conducted in a while. In some cases, the first steps may involve protecting against problems; in other cases, they may involve planning for the day when those problems arise. In general, though, a series of natural steps should be followed on a regular basis to ensure business risk mitigation:

1. **Assess risk.** Identify the factors that have caused downtime before and treat them as the start of your priority action list. They may include obvious causes, such as a missing UPS power supply, or other potential "weak links," such as the lack of a high-availability practice for minimizing downtime and data loss in the infrastructure. Other problem areas may include inefficient maintenance and data protection practices and inconsistent deployment of security patches or software upgrades across the organization. Office equipment, such as PCs and printers, that have inconsistent software updates, access controls, and data security measures may also be the cause of downtime and breaches, affecting user productivity and business operations. Don't underestimate the potential risks to be found in branch offices that may not have IT staff onsite, may not be running the most up-to-date software versions, or may not have implemented effective security measures to safeguard against unauthorized access.

2. **Measure the risk.** Managers need a way to gauge risk — to measure it in terms of dollar impact and time impact — over given intervals of time. Correlations must be made to tie the amount of downtime to the actual revenue loss experienced, even though this metric will vary by industry, by company size, and by workload. Build a consensus probability of a negative event (as in Figure 4) and estimate its financial impact. The product of the two will provide the expected negative value of the event for the time period under consideration.

3. **Identify the contributing factors.** A thoughtful analysis of downtime can reveal a wide array of possible causes: hardware, software, maintenance practices, power/cooling within the datacenter or computer room, and network connectivity — along with natural disasters and power outages. Using calculators that are built around reported linkages between risk factors and downtime can help business managers evaluate risk in their IT infrastructure.

4. **Evaluate options for reducing risk.** This is what risk mitigation is all about, of course — developing a plan that counters the causes of downtime given the methods proven in customer sites, such as replication of production data, use of high-availability software, and presence of alternate computing resources such as more computers or more storage devices to use as needed.

5. **Implement mitigation solutions.** Work with a third-party advisor (e.g., vendor, systems integrator, consultant) to find appropriate mitigation solutions based on long-term observations relating specific risk factors to resultant downtime. Experience in working with such factors, and the technologies that reduce risk related to those factors, will help your firm prioritize the list of solutions that can be brought to bear to reduce business risk related to systems outages. The third-party approach may seem unnecessary given that you know your company best, but the reality is that a fresh set of eyes can see things you may be missing. Plus, experience working with other firms similar to your own in size or industry can add a whole new layer of insight moving forward.

6. **Monitor and evaluate.** A full evaluation will help managers to rank the company's priorities — in the order in which they must be addressed. Results from putting a plan into action must be monitored, over time, to refine the plan itself — and to improve its effectiveness in combating business risk. Risk mitigation is a process, not a destination, and must be tended to on a continuing basis.

CHALLENGES

The market for IT products and services is a competitive one. With regard to business risk, and IT infrastructure downtime, no one vendor's solutions may encompass, or address, all the causes of downtime. For that reason, customers should take a comprehensive look at a wide array of possible factors contributing to system downtime. There are likely to be multiple "answers" to the question of "How do I reduce business risk in my organization?" However, systems vendors have likely developed an ecosystem of value-added resellers, systems integrators, and others to help provide an "outside" view of how to best protect their infrastructure (e.g., servers, storage, network).

The second, perhaps more daunting challenge to risk mitigation is internal. There is an element of self-criticism associated with problem identification, especially if IT managers who helped design and implement potentially vulnerable systems are still around. Clearly, the message to everyone needs to be "fix the problem," not "fix the blame." Management must resist the temptation to criticize decisions that have brought the IT environment to its current state and instead honestly appraise strengths, weaknesses, and next steps. Senior management support of this approach is essential for success.

CONCLUSION

Midsize companies are now suffering from a wide variance of system failure rates. These failures feed into operating income loss. But the means to identify and manage the risks of these losses exist. Those firms at risk need to know it, measure it, and mitigate it. The midsize firm not only must look carefully at its operations to find new efficiencies, apply new technologies, and implement new approaches to improve but also must identify from a holistic perspective where vulnerabilities reside and implement programs to manage them. The results will pay continuing dividends to the organization.