

THE BUSINESS CASE FOR DISASTER RECOVERY PLANNING: CALCULATING THE COST OF DOWNTIME

WHAT IS THE IMPACT OF DOWNTIME?

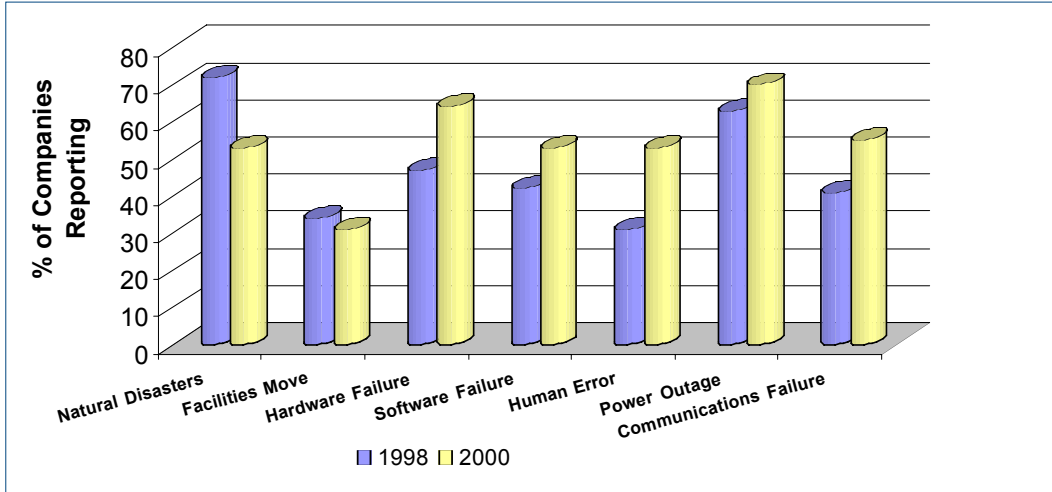
Over the past 20 to 30 years, businesses of all sizes have steadily grown more dependent on their expanding IT infrastructures to help them automate, manage, and analyze their business operations and strategy. Whether it's online trading, insurance-document imaging, airline reservations, financial databases, Web sites, or other computing systems, the fortunes of business are inextricably linked to the continuous availability of these services and data.

Unfortunately, IT infrastructures face varying risks of interruption. Most executives focus on natural disasters such as hurricanes, tornados, floods, and earthquakes. But IT leaders recognize that a disaster can be any event that prevents a business from accessing the data and systems it needs to operate. That could encompass everything from regional power outages, to virus outbreaks, to employee sabotage, to external data fraud, to devastating terrorist attacks.

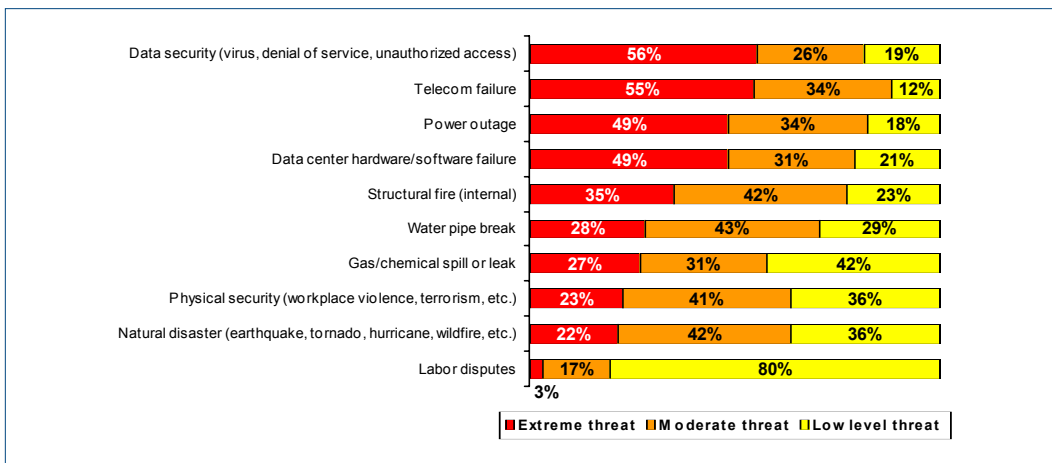
It's human nature to look at these risks and assign a very low probability to their occurrence in your business. But that simply isn't the case: virtually every company faces the risk of IT interruptions that can grind business to a halt. A KPMG study conducted in the millennium showed the shifting nature of these interruptions with natural disasters comprising a shrinking portion of the total causes of IT interruptions and manmade disasters — human- and IT-related failures — representing an increasing share.

¹"Contingency Planning & Management/KPMG Business Continuity Planning Survey," cited in Andy Hagg, "BCP on the Rise," Contingency Planning and Management, January 2001

TABLE OF CONTENTS	
WHAT IS THE IMPACT OF DOWNTIME?	1
HOW IRON MOUNTAIN OFF-SITE DATA PROTECTION CALCULATED THE COST OF DOWNTIME	4
STEP 1: Identify the Business Continuity Components That You Will Focus On	4
STEP 2: Define What You're Protecting	4
STEP 3: Prioritize Business Functions	5
STEP 4: Classify Outage Types, Frequencies, and Duration	6
STEP 5: Calculate the Cost of Downtime	8
SUMMARY/CONCLUSION	11
BIBLIOGRAPHY	12



A recent² survey of the members of the New England Disaster Recovery Information X-Change (NEDRIX) confirmed the prevalence of man-made events as the primary threats to business continuity.



Listed above are types of events that may pose a threat to business continuity at your organization. Using a 10-point scale, where '10' means that the event poses a 'extreme threat' and '1' means that the event 'does not pose a threat,' please rate the events on the level of threat each poses.

² "Top Business Continuity Priorities for 2004," ©EnvoyWorldWide - February, 2004.

The business implications of these disasters couldn't be starker. A frequently cited study in *Contingency Planning and Management* magazine found that 40 percent of companies that shut down for three days failed within 36 months. Depending on the industry and other factors, every hour of computer downtime can cost businesses from thousands — to millions — of dollars. Given the stakes, most companies believe that disaster-recovery planning and preparedness are non-negotiable requirements.

However, many technologists find it difficult to financially justify their requests for funding of disaster recovery planning and testing initiatives, despite their importance. In addition, many senior managers find it difficult to assess those requests in a business context. Of course, there's no such thing as an "average" business, so magazine statistics quantifying downtime costs are only marginally helpful.

A business impact analysis (BIA) can reveal the true costs of downtime and business disruptions for a particular business. However, these studies are expensive, and many executives are reluctant to spend money on a BIA without some way to measure the value or return on their financial investment (ROI). To show the value of a BIA and how to proceed, the following white paper outlines the steps for making a financial business case to justify disaster recovery planning and testing. The paper also describes how the Iron Mountain Off-Site Data Protection division calculated the cost of downtime for its own business and created a compelling ROI demonstration for disaster recovery planning and testing for its senior management team.

³ "2001 Cost of Downtime - Eagle Rock Alliance," *Contingency Planning and Management*

HOW IRON MOUNTAIN OFF-SITE DATA PROTECTION CALCULATED THE COST OF DOWNTIME

The following sections describe the process that one Iron Mountain division underwent several years ago in its initial effort to quantify costs associated with system downtime and create a financial estimate for justifying investments in preparedness. The process is still valid and useful and has been used in updated planning.

Step 1: Identify the Business Continuity Components That You Will Focus On

To create a comprehensive business-continuity plan, you need to assess the impact of downtime on four components:

- **People** — How will you notify, evacuate, transport, and care for employees (including, for example, paying them)?
- **Property** — What equipment will you need and how will you source it?
- **Systems** — What portions of your computing and telecommunications infrastructure must be duplicated immediately? Is that in a minute, an hour, or a day?
- **Data** — What data is critical to run your business — and how will you recover critical data that's lost?

In undertaking this project, Iron Mountain Off-Site Data Protection planners adopted a very conservative approach for calculating the impact of an outage. They knew that they could begin with systems and data and gather the information needed for these two components. They decided to start the process at this point and return to the people and property issues later.

Step 2: Define What You're Protecting

It's important to isolate the core competencies of your business and define what IT elements associated with those competencies must be protected. These competencies are the heart of what your business does and your unique proposition in the market - your competitive advantage. A core competency could be a product, service, process, or methodology.

When Iron Mountain looked at its business functions, it defined its core competency — or unique differentiator — as local service. Customers expect and receive great service from Iron Mountain because the company provides the resources of a large corporation through a locally empowered team. Given that emphasis, during disaster recovery for business continuity Iron Mountain IT should first focus on ensuring service levels on a local basis for all customers.

Step 3: Prioritize Business Functions

The next key step is to prioritize the business functions necessary to sustain that core competency in the face of a disaster or systems interruption. That means determining which data, applications, and systems get restored in what sequence and timeframes. Some systems have a high cost-of-interruption, which indicates that the business has a low tolerance for their interruption. Before categorizing systems as critical, vital, sensitive, or non-critical (i.e., to designate their degree of importance and order of restoration), make sure you interview your business users. They can help you test your hypotheses about which systems are business-critical and also can uncover overlooked systems.

Usually, a classic 80/20 rule applies. You'll typically apply 80 percent of your available resources to restoring the 20 percent of your systems, applications, and data on which your business depends most. For example, in a payroll-outsourcing company, the payroll processing system is the heart of the business and must be restored ASAP. For a shipping company, the package-tracking application is the critical system that must be restored immediately. Iron Mountain identified three systems:

- **Vault Management** — The company's primary operational system that manages off-site tape inventories and movement.
- **Customer-Facing Applications** — All hardware and software used by customers to retrieve information on their off-site data or to communicate with Iron Mountain about their account(s).
- **E-mail** — Iron Mountain's team concluded that e-mail was the number-one vehicle used by customers for communicating tape requests and other issues. It was considered crucial for customer service.

Step 4: Classify Outage Types, Frequencies, and Duration

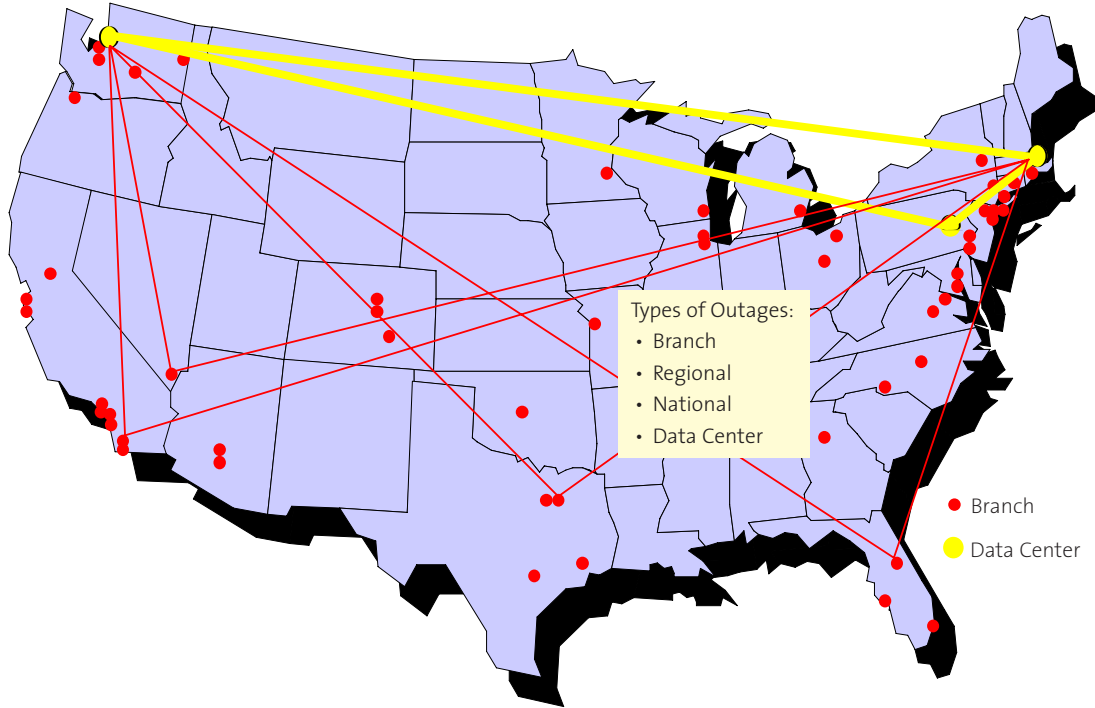
After you've prioritized the business functions, you'll want to analyze the hardware and software configurations that support those functions in order to understand their interdependence and find possible points of failure — and then quantify the hourly costs associated with systems interruption of those functions. To quantify hourly costs, you first need to know what types of outages you are likely to experience as well as their frequency and duration.

For example, Iron Mountain Off-Site Data Protection is geographically disbursed. At the time of the project, it operated three data centers spread across the country but connected by an ATM private high-speed network. The organization consisted of nearly 60 branch locations, each connected to two data centers in the wide area network to provide redundancy within the system. At a very high level, this was the computing infrastructure.

The Iron Mountain team worked with the IT Help Desk to obtain records of past branch outages. Its log of trouble tickets supplied much of the information needed. A pattern began to emerge as the team examined these records. Based upon the division's computing infrastructure, they identified four types of outages:

- **Branch Outage** — One of the division's branches goes down. This is the primary focus because a branch outage may impact Iron Mountain's ability to conduct business with local customers. Previous outages were, typically, caused by a faulty router, malfunctioning LAN, or loss of electrical power — only rarely by a natural disaster. These outages affected an average of eight branch offices once each month and, typically, lasted from one to four hours. After identifying these outage patterns, frequencies, and durations, the next step was simply to calculate the financial impact in order to find the information needed to build the business case for preventive investment. Iron Mountain then proceeded to do a similar analysis for each of the other types of outages. While each type of outages is different, the process of analysis is similar for each type.
- **Regional Outage** — This affects multiple branches within a single geographic region. Originally, Iron Mountain anticipated that these outages were most likely caused by natural disasters (e.g., a hurricane or flood) that would occur about once every three years. Analysis showed that, in fact, regional outages occur more frequently and are most often caused by telecommunication-company failures.
- **Data Center Outage** — This occurs when one of Iron Mountain's three data centers goes off-line. The team's analysis revealed that application failure — not fire, flood, or other catastrophe — was the biggest reason for a data center outage. Software bugs causing unplanned restarts were far more frequent than natural disasters. While the frequency and duration of data center outages are much lower than branch or regional outages, they affect all other sites in the network. For Iron Mountain's business, the team found that the most critical outages that needed to be addressed were the branch and data center outages.
- **National Outage** — This exceedingly rare event happens when the company's entire private, high-speed network goes down. The only recent example is the so-called "Black Monday" in 1999 when AT&T's telecom network failed nationwide.

CLASSIFYING OUTAGES: INFRASTRUCTURE



Step 5: Calculate the Cost of Downtime

One overlooked truth is that downtime costs accelerate in a non-linear fashion every hour. If a system fails for five minutes, the costs are fairly low because manual methods (paper and pencil) of making records or communicating by telephone instead of e-mails can suffice to conduct business. Over an extended period, however, the volume of work overwhelms the manual processes. Yet some businesses — such as Amazon or e-Bay — cannot run at all on manual processes. Business and financial operations increasingly deteriorate, and the rate of dollar losses grows — sometimes to the point of fatally damaging the business.

In addition, when assessing the financial impact of downtime, you need to consider factors such as potential lost revenue, reductions in worker productivity, and damaged market reputation. In some cases, downtime can even reduce shareholder confidence, which can create unnecessary and unplanned costs. Financial analysts and accountants at your company can help you come up with the factors at your company that are affected by downtime and contribute to its costs.

So, according to Iron Mountain's analysis, what does a one-day outage cost? The division experiences no direct short-term reduction in revenues and no significant expense for short-term productivity. Most transactions can be processed manually for a period of time, and Iron Mountain workers can catch up on transaction volume (through overtime hours) when normal operations resume.

The bulk of outage expenses identified arise from labor charges for a team of technologists who must resolve the outages. Other expenses included the cost of manually recording the 727,000 transactions recorded by the system each day, plus the cost of manually entering those transactions into the systems once they come back online.

Based on these transaction volumes, the Iron Mountain team calculated that a branch or remote office outage's cost was in the hundreds of dollars per hour. A division outage would cost tens of thousands of dollars per hour.

The Annual Cost of Downtime

Frequency x Duration x Hourly Cost = Lost Profits

Outage	Minimum Impact	Maximum Impact
Branch	1X	5X
Data Center	2X	10X
Regional	0.2X	1X
National	1.5X	1.5X
Total	3.5X	15X

Based on these results, Iron Mountain assigned this dollar value to a branch outage and calculated its total cost. If there were 90 branch outages in an average year each lasting an average of one-and-a-half hours and costing \$300/hour (based on the daily cost described previously, divided by the number of hours in a day), then the cost of branch outages for a year would be in the neighborhood of \$40,500. Expressed as an equation this is:

Branch Outage Cost = 90 outages per year averaging 1.5 hours each, and an outage cost of \$300 per hour or . . .

$$90 \text{ outages} \times 1.5 \text{ hours} \times \$300/\text{hour} = \$40,500$$

HOW MUCH DISASTER PREPAREDNESS CAN YOU AFFORD?

The previous chart is for demonstration purposes only. It doesn't contain specific dollar amounts, but, instead lists "orders of magnitude" in order to protect confidential Iron Mountain information. However, continuing with the Iron Mountain example, you can see how to create such a chart for calculating the cost of downtime for your own organization. What's more, you can use the data from that chart to calculate a financial rate of return on an investment in disaster preparedness.

For example, to make a conservative ROI calculation in the case of Iron Mountain, consider the average cost of branch downtime calculated earlier at \$40,500 to be the "1X Minimum Impact" cost for this chart.

Then assume that rarely — but occasionally — an incident occurs in which branch outage costs for a particular event are unusually high. Even if that event won't happen for six or seven years, you probably want to include such infrequent outages in your financial cost calculations since they will be included in total costs over longer periods of time. In the Iron Mountain example, this is included as the "5X Maximum Impact" -and would be \$202,500 ($\$40,500 \times 5$).

Building such a chart for your own business, using documented historical outages or conservative estimates if historical data is not available, helps you to calculate the multi-year financial impact of outages. You can then calculate a payback period for any investment to offset those five-year costs by using guidelines provided by your accountants, such as a three-year or five-year payback period.

If you use a three-year payback period, you can now demonstrate that there is solid payback evidence for any investment that is up-to-three times the annual cost of the downtime you have been calculating. For a five-year period, you can demonstrate the ROI for an investment of up-to-five times the annual cost of your downtime. Using this process, you can build a business case to justify investment in disaster preparedness, disaster recovery planning, and testing.

Iron Mountain Off-Site Data Protection created a business case using this type of process and successfully obtained funding for its own disaster-recovery initiatives.

SUMMARY/CONCLUSION

Given the potentially enormous long-term costs and implications of a business-systems interruption, companies need to carefully define and implement plans to mitigate the costs. Building the case for investing in disaster recovery/business continuity begins with defining what functions are critical to your business and tying that to the key systems that support those functions.

Once you've identified those systems, you need to analyze your hardware and software configurations to understand their interdependence and find possible failure points. Next, track your outages, identify their causes, and correlate them to possible points of failure that you've identified. Then determine the frequency and duration of these outages and identify which points of failure cost your business the most. You need to assign costs to these points of failure and manage these costs to maximize the ROI and minimize the losses felt by the entire organization.

Finally, disaster preparedness and recovery planning are iterative processes — not a discrete, one-time event. Enterprises should take care to continually revisit their disaster-recovery plans to ensure they remain aligned with current business realities and goals and to test those plans regularly to ensure that they perform as planned.

For additional information about disaster recovery services and testing as well as online backup and off-site data protection, visit www.ironmountain.com

BIBLIOGRAPHY

- References:

- *Disaster Recovery Planning: 3rd Ed.*

Jon William Toigo (author), Prentice Hall PTR, 2003

- Publications:

- "Top Business Continuity Priorities for 2004" © EnvoyWorldWide
- *Contingency Planning and Management*
- *Disaster Recovery Journal*

About Iron Mountain

Iron Mountain Incorporated (NYSE:IRM) is the world's most trusted partner for outsourced records and information management services. Founded in 1951, the Company has grown to service more than 150,000 customer accounts throughout the United States, Canada, Europe and Latin America. Iron Mountain offers records management services for both physical and digital media, disaster recovery support services, and consulting - services that help businesses save money and manage risks associated with legal and regulatory compliance, protection of vital information, and business continuity challenges.

Iron Mountain

Off-Site Data Protection Services
745 Atlantic Avenue
Boston, MA 02111
(800) 962-0652
www.ironmountain.com