

Forrester Consulting

HELPING BUSINESS THRIVE ON TECHNOLOGY CHANGE

Workforce Continuity: Keeping People Productive During A Workforce Disruption Or Disaster

A commissioned study conducted by Forrester
Consulting on behalf of Citrix Systems
August 2006

FORRESTER®

FORRESTER®

Headquarters

Forrester Research, Inc., 400 Technology Square, Cambridge, MA 02139 USA
Tel: +1 617/613-6000 • Fax: +1 617/613-5000 • www.forrester.com

Introduction: Preparing For A Workforce Disruption

During business continuity planning, more attention is given to continuing data center operations in the event of a disaster or disruption than anything else. But business continuity (BC) encompasses more than just data center continuity: It encompasses all resources, IT assets, and *people* that are necessary to continue critical business operations in the event of a disruption. New threats that affect people more than they affect IT assets, such as pandemics and transit strikes, are forcing enterprises to realize that, while they have taken extraordinary measures to protect and continue data center operations, they have not taken the necessary steps to ensure that their people can continue to have access to their applications, data, and communication (email, messaging, voicemail, fax etc.) in order to remain productive.

The study commissioned as part of this report shows that a major workforce disruption can cost millions of dollars in lost productivity. As an example, a 5,000-person enterprise, with a large percentage of its workforce centrally located at a single corporate facility, would suffer a \$1.36 million productivity loss as a result of three-day workforce disruption. In this age of 24x7 operations, increased competition, and heightened customer expectations, enterprises must do more than restore the data center and resume only critical business operations: Enterprises must reconnect as many people as possible back into the firm as quickly as possible to maintain productivity as well as the competitive edge. Knowledge and service industries — such as financial services, professional services, and high-tech — are particularly vulnerable to workforce disruptions because they rely heavily on the intellectual capital and customer service of its people to conduct business.

Enterprises now recognize that they must modify their business continuity plans and budgets to include strategies and solutions for “workforce continuity.” Over time, Forrester expects that enterprise spending on “workforce continuity” (WC) could approximate the current spending on data center continuity.

Forrester defines workforce continuity as:

A strategy that provides for connecting a dispersed workforce to the applications, data, and communications they need in instances where pandemic, transit strike, natural disaster, or other events prevent the workforce from reaching a corporate facility.

Citrix commissioned this study to determine the following:

- The current state of overall disaster recovery and business continuity efforts.
- The level of current preparedness of enterprises to reconnect all workers to their applications, data, and office communication during a workforce disruption or disaster.
- The level of demand from enterprises to simply and effectively link their workers back to the tools that they need in order to be productive during a disaster or other workforce disruption.
- The costs associated with having an employee out of the office and unconnected.

Study Methodology

In summer 2006, Forrester Consulting conducted an online survey of 250 IT decision-makers and influencers across North America and the United Kingdom. In this survey:

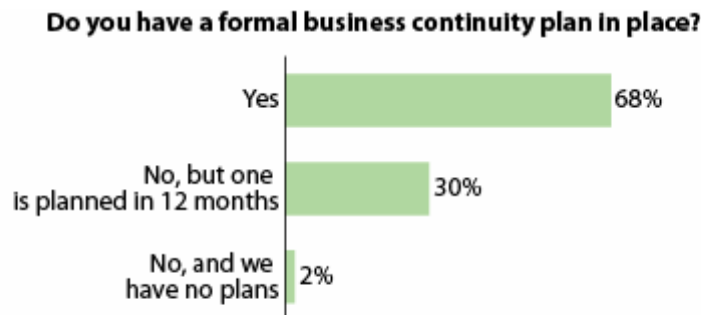
Workforce Continuity

- Sixty-six percent of respondents were from North America (United States and Canada), and 34% were from the UK.
- Thirty-six percent of respondents were from enterprises that had 1,000 to 4,999 employees, 44% had 5,000 to 19,999 employees, and 20% had 20,000 employees or more.
- Thirty-three percent of respondents were from companies with revenues of \$250 million to \$750 million, 33% were from companies with revenues of \$750 million to \$1.5 billion, and 33% were from companies with revenues greater than \$1.5 billion.
- All respondents were technology decision-makers or influencers for operational risk management, disaster recovery, or business continuity. Eighty-six percent of respondents had a title commensurate with director or above such as manager or director of IT, VP of IT, or CIO.
- Respondents were from a variety of knowledge- or service-based industries such as retail, financial services, professional service, high-tech, and government.

Market Overview: The State Of Business Continuity Preparedness

Approximately 68% of respondents spend more than \$3 million on business continuity, showing that business continuity budgets (budgets for labor, technology, and services) are healthy. But surprisingly, 32% do not currently have a business continuity plan in place. Thirty percent plan to develop a formal business continuity plan in the next 12 months, and 2% never intend to develop one at all (see Figure 1).

Figure 1: Formal Business Continuity Planning



Base: 250 business continuity/disaster recovery decision-makers

Source: A commissioned study conducted by Forrester Consulting on behalf of Citrix, August 2006

It is important to develop a formal plan: Enterprises without a formal business continuity plan have no way to recover from a major disruption or natural disaster in an organized manner, which is key to minimizing the downtime and revenue loss. In a world where enterprises increasingly depend on external partners and Web applications for day-to-day operations, proof of business continuity planning is increasingly a prerequisite for trusted suppliers and partners. Formal business continuity planning consists of the following three phases:

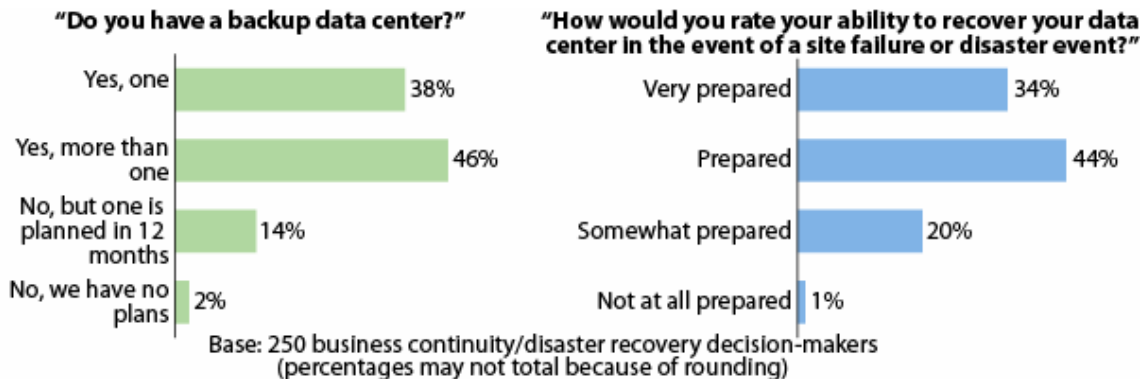
- **Business impact analysis (BIA).** During the BIA, enterprises must identify the most critical business operations and the dependent resources. Resources include not only IT

assets, but non-IT assets, human resources, business partners, suppliers, service providers, etc. Also during this phase, enterprises define their recovery time and recovery point objectives for each critical business operation.

- **Local threat assessment.** During this phase, enterprises develop a local threat profile by identifying the specific threats it must protect itself against. What threats can the enterprise anticipate? What is the history of natural and manmade disasters for the local region? Also, the enterprise must identify the more mundane (but likely) threats that preventative measures can protect the primary data center against, such as power and network failures.
- **Business continuity plan development and maintenance.** The development of the BC plan itself consists of a local site hardening (reinforcing building integrity and security, dual-generators, creating redundancy in IT assets and network infrastructure), an emergency communication strategy, data center continuity strategy, workforce continuity strategy, backup data center site selection, technology selection, etc. It also includes a strategy for testing and ongoing plan maintenance.

Most enterprises focus on restoring IT assets in the event of a business disruption. According to the survey, on average, 30% of the business continuity budget is allocated to data center continuity, and more than 84% of respondents have at least one backup data center while another 14% of respondents plan to have one in the next 12 months. Yet despite these efforts, enterprises are not entirely confident in their ability to recover the data center in the event of site outage or natural disaster — only 34% of respondents describe themselves as “very prepared” (see Figure 2). Forrester attributes this to the fact that 32% of respondents don’t have a regularly maintained and tested formal business continuity plan in place to help direct the recovery of all dependent resources during a disruption.

Figure 2: Data Center Continuity Preparedness



Source: A commissioned study conducted by Forrester Consulting on behalf of Citrix, August 2006

Workforce Continuity Preparedness

In addition to planning for data center continuity, new threats, such as pandemics, have forced enterprises to re-evaluate their workforce continuity strategies. What is unique about these events is that the data center is unaffected, but the workforce is unable to get to a corporate facility.

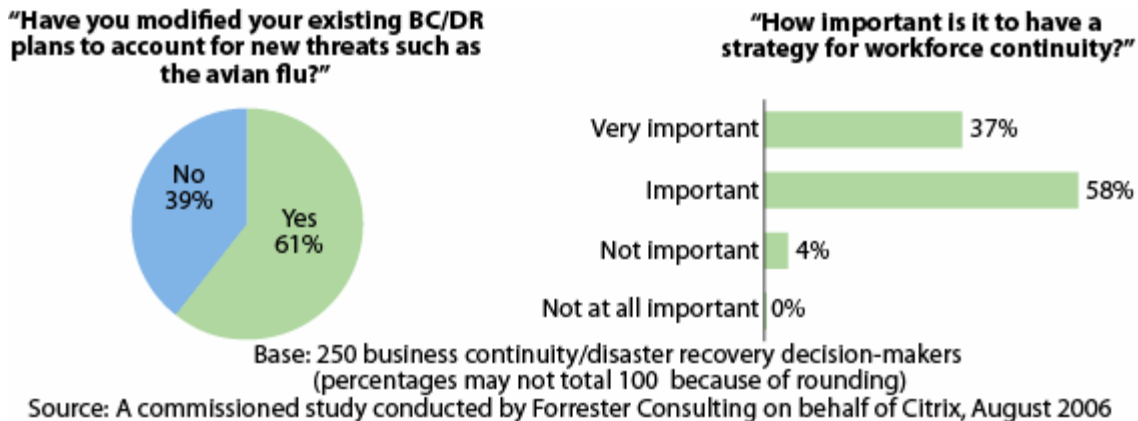
The growing importance of developing a workforce continuity strategy along with data center continuity as part of a comprehensive BC plan is already underway.

- Sixty-one percent of respondents have already modified their BC plans to account for new threats such as avian influenza (bird flu) (see Figure 3).

Workforce Continuity

- Approximately 95% of respondents believe it is “important” or “very important” to have a workforce continuity strategy in place.
- Sixty-three of respondents currently have a workforce continuity strategy in place as part of their BC plan and another 32% plan to include one in the next 12 months.
- Sixty-one percent of respondents report that their business continuity plan includes an emergency communication and notification strategy or plan, and 34% plan to include one in the next 12 months.

Figure 3: Workforce Continuity Criticality



Despite these initial efforts, enterprises are not yet fully prepared for a major workforce disruption. Only 25% of respondents rate their ability to recover from a workforce disruption as “very prepared.” This is 10% below the number of enterprises that rate themselves as “very prepared” to recover their data center. Forrester attributes this low preparedness rating to the fact that a large percentage of respondents do not have a formal strategy for workforce continuity in place, coupled with the fact that many respondents don’t have an umbrella plan to direct all business continuity efforts during a disruption or crisis.

Market Analysis: Workforce Continuity Demands And Strategies

When it comes to workforce continuity, there are three key capabilities that a comprehensive strategy includes:

1. A formalized emergency communication and notification system linking the organization and workers enabling the delivery of key communication from the enterprise and to track worker status.
2. Continued access to key business applications, such as email, ERP and CRM systems, and end user data to keep critical business operations running.
3. Continued access to full office communications, such as office phone, voicemail, and collaboration tools, so workers can communicate inside and outside the organization.

When enterprises were asked to rank the importance of these capabilities to their workforce continuity strategies on a scale of 1 to 4, where 1 is not all important and 4 is very important,

Workforce Continuity

enterprises ranked emergency communication the highest (3.5), followed by access to business applications and data (3.4) and access to full office communication (3.2). The closeness of these rankings indicates that enterprises generally regard all three of these capabilities as essential to their workforce continuity strategies.

There are 3 major categories of workforce continuity solutions:

- **Solution 1:** Organization either contracts with a third-party provider for workspace or provisions its own workspace in an alternate location to provide necessary space and resources (desktops, local area network (LAN), phone, private branch exchange (PBX), call management system, etc.)
- **Solution 2:** Organization contracts for mobile workspace trailers with the necessary space and resources to be located in a parking lot or at another predetermined location. Communications are provided through very small aperture terminal (VSAT) links until land lines are secured.
- **Solution 3:** IT creates standard remote-access procedures such as virtual private networks (VPN), SSL VPN, remote application presentment, and remote desktop access solutions. These solutions enable employees to remotely access corporate applications and data from home or some other location until the primary facility is restored or relocated.

Solution 3, creating standard remote-access procedures, is an increasingly popular alternative because it is low-cost, and many enterprises already have a remote-access infrastructure in place. Enterprises can build on this infrastructure foundation by formalizing an emergency communication and notification plan, as well as adding specific remote-access solutions and communication and collaboration solutions as necessary and appropriate. The appropriate remote-access solution (VPN, remote application presentment, remote desktop access) will depend on whether individuals work with laptops or desktops in the office, and whether they have personal PCs at home. According to our survey of workers who currently have remote access from home, 44% use a personal laptop or desktop. The other advantage of this solution is that it makes much more sense in a situation where workers might not be able to travel at all — such as during a pandemic when workers may be prohibited from travel, or during a transit strike when workers are unable to travel to a corporate facility.

Solutions 1 and 2 will likely not provide enough space for the entire workforce. For example, most third-party service providers have a limited number of spaces for a given region, and these spaces are often oversubscribed (meaning that they have been sold to several enterprises). This means that during a regional disruption or disaster, the first enterprise to declare a disaster will have access to the available seats. Solutions 1 and 2 are more appropriate for specific individuals (call centers, emergency response teams, etc) but not as a solution for the entire workforce.

Workforce Continuity: Spending

Eighty-six percent of respondents indicated that spending on workforce continuity would come from existing business continuity budgets. Figure 4 shows that the amount enterprises currently spend or intend to spend on workforce continuity correlates closely with size of the existing business continuity budget (see Figure 4). The data also indicates that enterprises “intend” to spend as much as 30% of their business continuity budget on workforce continuity — this approximates what enterprises currently spend on data center continuity.

Workforce Continuity

Figure 4: Planned Workforce Continuity Spending Correlates To Business Continuity Budget

"How much do you intend to spend on workforce continuity?"

		Existing business continuity budget							
		Less than \$500K	\$500K to <\$1.5M	\$1.5M to <\$3M	\$3M to <\$6M	\$6M to <\$10M	\$10M to <\$20M	\$20M to <\$50M	Greater than \$50 million
Planned workforce continuity spending	Less than \$250K	79%	29%	9%	4%	0%	3%	0%	5%
	\$250K to <\$500K	14%	45%	29%	12%	3%	5%	0%	5%
	\$500K to <\$1.5M	0%	16%	40%	50%	34%	8%	18%	10%
	\$1.5M to <\$3M	0%	6%	14%	24%	49%	38%	14%	10%
	\$3M to <\$6M	0%	0%	0%	4%	11%	38%	61%	15%
	Greater than \$6M	0%	0%	0%	0%	0%	5%	7%	55%
	Don't know	7%	3%	6%	6%	3%	3%	0%	0%

Base: 250 business continuity/disaster recovery decision-makers

Source: A commissioned study conducted by Forrester Consulting on behalf of Citrix, August 2006

Whether or not enterprises have an accurate estimate of how much they intend to spend on workforce continuity, it's clear from this study that workforce continuity is important to very important to enterprises and that enterprises will need to fund their solutions from their BC budget. This means that enterprises will need to increase their business continuity budget or, in some cases, shift some of the budget to workforce continuity preparedness from other initiatives. However, many enterprises have existing investments in other workforce productivity solutions that can be coalesced into workforce continuity strategy and coordinated with the umbrella BC plan.

On average, 36% of an enterprise's workforce currently has remote access to company applications and data from home. Enterprises indicated that in order to continue business operations, 38% of the workforce would absolutely have to have remote access. The similarity of these percentages indicates that enterprises have — at most — focused their workforce continuity efforts to date on attaining only a basic level of preparedness. While this effort is an important first step as enterprises have come to appreciate the importance of workforce continuity, the next step will be to expand coverage to a greater percentage of the workforce and to add more robust capabilities, such as full access to office communication and collaboration tools for increased productivity.

Through a business impact analysis (the first phase of business continuity planning), enterprises identify all the resources (people and IT assets) that are necessary to continue or resume critical business operations. This essential planning minimizes revenue loss but does not completely mitigate the costs of lost worker productivity or lost market share. Lost worker productivity can cost millions in this age of 24x7 operations, increased competition, and heightened customer expectations. In this environment, it is not enough to simply continue or resume only the most critical business operations. Mitigating crisis-related losses involves maintaining the same level of uninterrupted customer service customers are accustomed to. Degraded customer service creates customer churn and an opportunity for competitors to seize market share. Reconnecting as many workers as possible (at a reasonable cost) to their applications, data, and communication tools is now the goal of workforce continuity.

Calculating The Cost Of Lost Worker Productivity

Enterprises often calculate the cost of downtime based on lost revenue alone. While this is an important calculation to include, it is not the only measure of the cost of downtime — lost productivity must also be included. During a disaster or business disruption, you must still continue to compensate your workforce and cover its benefit costs even while the workforce is unable to work. This is a significant loss to the enterprise. Enterprises can use the following calculation to determine the cost of lost worker productivity:

[# OF WORKERS AFFECTED] X [# OF HOURS OUT] X [BURDENED HOURLY RATE]

The [# OF WORKERS AFFECTED] is the number of workers who are likely to be affected by a given disruption. According to our survey, on average, 38% of an enterprise's workforce works at a single company facility. This means that 38% of the workforce could be affected by a single disruption.

The [# OF HOURS OUT] is the number of hours that workers are unable to go to a corporate facility to conduct business. For example, in December 2005, a transit strike disabled New York City's subway system for more than three days, leaving thousands of people searching for alternate means into the city or not going into work at all.

The [BURDENED HOURLY RATE] is the hourly cost per worker including salary plus benefits. According to our survey, the annual cost per worker (including salary and benefits) is \$72,848, and the average work week is 46.7 hours (or 9.34 hours per day). Therefore, the average burdened hourly rate is \$30 per hour.

So as an example, suppose the workforce of a 5,000-employee enterprise was disrupted by the transit strike. Using the averages from our survey, it's likely that 1,900 employees were directly affected the disruption (because on average, 38% of workers work at a single corporate facility) and they were unable to report to work for three business days, which translates into a productivity loss for the company of approximately \$1.36 million ([1,900 employees] X [28 hours out] X [\$30 per hour]). If our example enterprise follows the average and 36% of its workforce has remote access from home, then this would reduce the number of workers affected to 1,216 and the productivity loss to \$875,000.

So enterprises can take the route of ensuring that the bare minimum of workers have remote access, or it can try to ensure that the greatest number of workers at a reasonable cost has remote access and thereby greatly reduce its productivity loss.

Conclusions

The objectives of this study were to understand the current state of business and workforce continuity preparedness, demand for solutions that address workforce disruptions, and the costs associated with productivity loss. The study's findings can be summarized as follows:

- Enterprises have made strides in overall business continuity preparedness and data center continuity preparedness, but there is still room for improvement. The majority of enterprises either have or are planning to have a backup data center, but 40% of enterprises are still in the process of developing a formal business continuity plan, and only 36% of enterprises rate themselves as "very prepared" to recover their data center. While enterprises have clearly made significant investments in business continuity/disaster recovery technology, without formal plans and regular and consistent testing, successfully executing a data center recovery in an orderly manner is likely difficult for most enterprises.

Workforce Continuity

- While a majority of enterprises (61%) have already adjusted their business continuity plans to account for new threats such as avian influenza (bird flu) and a majority of enterprises (63%) currently have a workforce continuity strategy in place, only 25% of enterprises feel that they are “very prepared” to reconnect workers in the event of a major workforce disruption. Despite recognition of the need for workforce continuity and some adjustments to provide for it, enterprises must develop more formal plans and improve their overall preparedness.
- The level of demand for workforce continuity solutions is very strong, given how highly enterprises rated the importance of having a strategy in place. Over time, enterprises expect to spend almost as much on workforce continuity as they currently do on data center continuity. To achieve this, enterprises will need to increase overall business continuity spending or shift existing spending from other initiatives to workforce continuity.
- The costs associated with having a worker out of the office and unconnected to business applications and data are significant, given that the average burdened hourly rate is \$30 per hour. With an average of about 38% of responding enterprises’ workforce based at a single corporate facility, a single disruption or disaster has the ability to create considerable productivity loss if the enterprise does not have a workforce continuity strategy in place. As an example, a 5,000-person enterprise would suffer a \$1.36 million productivity loss as a result of three-day workforce disruption. The same 5,000-person enterprise with 36% of its workers having remote access from home would reduce its productivity loss to \$875,000. So the more people an enterprise can keep connected and productive, the more it can reduce its productivity loss, and the more competitive it’s likely to remain during the disruption.

Enterprise Recommendations

- **Develop a business continuity plan.** If your enterprise doesn’t have a formal business continuity plan in place, this needs to be one of your highest priorities in the next six months. Without a formal plan in place, it will be difficult to coordinate recovery efforts during a business disruption or disaster — if you’re lucky to recover successfully at all. A formal plan will allow you to identify your most critical business operations and dependent resources; the threats you need to protect against; preventative measures to help avoid the most likely threats; and the people, technology, and process necessary to actually execute recovery. In addition, you’ll increasingly find that having a formal BC plan in place is a prerequisite for many business partners.
- **Include a workforce continuity strategy in your business continuity plan.** A comprehensive business continuity plan must include a strategy for keeping workers productive during a disruption or disaster. While data center continuity is an important part of your overall BC plan, it is just one element of the plan. New threats such as pandemics increasingly affect the workforce more than the data center itself — you must account for these new threats alongside your data center continuity strategy.
- **Determine the cost of lost worker productivity.** The cost of downtime is more than just lost revenue: It also includes the cost of lost worker productivity. Calculating lost worker productivity will help you understand your potential financial losses in the event of a major workforce disruption, and it will help you justify additional investment in workforce continuity solutions to senior management. The more workers that you can provide with remote access to corporate applications and data at a reasonable cost, the more you can reduce your productivity losses and also maintain your current level of customer service.