

WHITE PAPER

Ensuring Enterprise Workforce Continuity

Sponsored by: iPass

Stacy K. Sudan

April 2007

INTRODUCTION

Workforce Continuity Is an Essential Component of Business Continuity

Today's economic reality is that businesses are expected to be up and running 24 x 7. This requirement stems from the fact that many companies have resources, customers, and suppliers spread out across the world and is also due to the emergence of the Internet as an always-available marketplace.

This requirement has raised the cost of business downtime, whether caused by natural disasters, political instability, or simply bad weather. It also has spawned heavy interest in business continuity planning, with a focus on IT assets and systems that ensure that online systems continue to function at all times. Until recently, businesses have been shortsighted about the role of people in the business continuity equation — not enough attention has been focused on how to ensure that the workforce that operates these systems can actually do so in the event that a local or regional disruption shuts down their primary work location.

The lack of a strategic approach to address this neglected area, which we call "workforce continuity," leads to incomplete business continuity plans that put a company's operations, reputation, and financial livelihood at risk.

The enablement of remote and mobile work for all critical workers is an essential component of a workforce continuity strategy. The Internet and rapid advancements in mobile communications and device technologies have made it possible for companies to create a virtual office for their employees so they can work from anywhere at any time. This mobility not only can increase productivity in general but also provides a platform for workforce continuity in the face of interruptions large or small. IDC research estimates that in 2006, mobile workers accounted for 25% of the worldwide worker population, or 744 million workers (see *Worldwide Mobile Worker Population 2005–2009 Forecast and Analysis*, IDC #34124, October 2005).

A workforce continuity strategy ensures that employees, regardless of their location, have a way to connect to the critical systems and resources that they need to conduct business. A key question businesses need to consider is how to cost-effectively enable workers who perform operationally critical jobs — especially those who solely or primarily work from the office during normal operations — to be prepared for a disaster or interruption.

Until recently, businesses have been shortsighted about the role of people in the business continuity equation. The enablement of remote and mobile work for all critical workers is an essential component of a workforce continuity strategy.

DRIVERS FOR BUSINESS CONTINUITY

Businesses Need to Find a Predictable Solution for Unpredictable Events

A number of potential events can cripple workers in certain locations. These events can be categorized as disasters and interruptions.

The most sensational events are disasters, which often occur suddenly and have broad impact across a geographic area with little warning. The impending impact of these events is often poorly understood. Recent examples include the hurricanes of 2005 and the Taiwan earthquake in December 2006. Another example is the likelihood of a major pandemic or epidemic in the coming years, which has the potential to force quarantine conditions and a remote work environment. Closely related are man-made calamities such as the 9/11 terrorist attacks and other acts of war. Clearly these events can take key locations completely offline and force everyone into a "remote and mobile" mode of operation for an extended period of time.

Less devastating, but potentially as much of a drain on productivity when considered in aggregate, are the myriad disruptions that impact smaller groups for shorter periods of time. These disruptions include weather events such as snowstorms, heat waves, and flooding as well as man-made events such as transit problems, power outages, strikes, and political protests. Each event may seem to be a minor inconvenience in isolation, but the total effect of such events on a company's bottom line can be just as harmful as the effect of a sensational event.

Although these types of events are not new to the world, their impact on a company's performance has been magnified by the movement of processes to online systems and the increasingly interconnected nature of the global and mobile workforce.

Companies have spent the past decade using technology to eliminate jobs that consist of rote activities, but the workers who remain are more critical than ever before, using online systems to communicate, assess information, and make decisions that keep their companies up and running. Because these online systems allow employees who perform critical functions to be dispersed all over the world, businesses need to ensure that workers in all locations have access to a solution that allows them to keep working in the face of disaster. Companies rely very heavily on technology today, but employees provide the valuable skills that keep companies up and running.

Businesses need to ensure that workers in all locations have access to a solution that allows them to keep working in the face of disaster. Companies rely very heavily on technology today, but employees provide the valuable skills that keep companies up and running.

SUCCESS FACTORS AND DEPLOYMENT CONSIDERATIONS

Critical Success Factors for a Workforce Continuity Solution

When choosing a workforce continuity solution, businesses should look for certain attributes that will help ensure the success of the solution after it is deployed. If any of these key components are missing, the strategy might not be able to meet their needs.

Ideally, a workforce continuity solution should include the following characteristics:

- Usable regardless of worker location; supports an array of access methods from inexpensive and highly available to faster yet less plentiful
- Usable over a broad array of user device types including home desktops, laptops, PDAs, and smartphones
- Built-in redundancy so that availability is not tied to a single point of failure
- Can scale "instantly" in the face of a widespread displacement of workers
- Meets security requirements as defined by IT for an emergency situation (The requirements may be less stringent than those that normally apply to ensure the business can continue to function.)
- Easy for IT to deploy as standard equipment to workers
- Easy for IT to maintain and test during periods of normalcy
- Highly intuitive for the end user with only minimal training
- Includes service-level agreements to ensure clear understanding of what the service delivers during different types of outages
- Priced reasonably to enable all employees to use the services during periods of normalcy, as well as in case of emergency

Considerations for a Successful Workforce Continuity Deployment

Companies need to consider multiple factors when planning a workforce continuity strategy.

A companywide evaluation should be performed with the goal of looking at different operational groups and determining how critical each group is to the company's bottom line in a time of crisis or disruption. Groups and processes should fall into one of the following three categories for restoring connectivity:

- Essential to serving existing customers (high short-term impact)
- Essential to capturing new customers or extending customer relationships (medium short-term impact)
- Everything else (low short-term impact)

One of the first steps in evaluating workforce continuity needs should be to segment workers by the criticalness of their role to *business operation* during an outage. In an emergency situation, various roles in a company may take on different levels of importance than they would during normal operations as an organization is forced to focus on basic tactical execution while waiting out the interruption. For this reason, in a disaster, a customer-facing role such as a customer service representative or field technician may be much more important to get back online than an inward-facing role such as a software engineer, a factory foreman, or normally strategic personnel such as nonoperational executives.

In addition to worker segmentation, companies need to carefully evaluate their business processes. When performing a companywide evaluation, businesses should review their different operational processes and determine how critical each is to maintaining revenue flow and customer satisfaction — the two factors most at risk during an outage. After gaining a full understanding of the steps in each process, companies should determine the best way to ensure that the correct flow can be maintained in case employees are dispersed. As part of this evaluation, companies should also look at all their operational groups and the resources they have in place to deploy the continuity solution. Employees who are on the road much of the time, such as salespeople or executives, are likely to have laptops and may be familiar with connecting to the corporate network while outside the office. Employees who are usually in the office, such as administrative or human resources employees, may not have laptops or a high degree of comfort with connecting over mobile networks.

Then companies should consider what resources and applications different employees need to access in order to conduct these processes. The systems that a software engineer requires may vary widely from those needed by a customer service representative or a middle manager. These needs will allow companies to determine the technologies required to provide access in case of an emergency, such as overall and per-user bandwidth and latency requirements, and to determine if Web applications will suffice or if full VPN access is required. Companies also need to consider that their operations teams may need to be able to manage these systems remotely as well.

Deployment Steps:

- 1) Segment workers
- 2) Evaluate business processes
- 3) Determine which resources are required by each segment of workers
- 4) Evaluate locations from which access might be needed
- 5) Ensure employees are trained and use the continuity solution regularly

In addition, companies should carefully evaluate the different locations from which critical employees will need to get access during an emergency or a disruption. Employees' homes may be among the most important places from which they require access to corporate systems. It is important to also consider that employees can just as easily be away from home when an incident occurs and may be in airports, hotels, or other locations. Or the disaster may keep them away from home for an extended time. Certain countries or locales may be identified as important even if they do not host a formal corporate office. Ensuring that users have a secure, reliable connection to the Internet from any of these places is essential to the success of a workforce continuity solution.

Another important element of a workforce continuity strategy is ensuring that employees are trained on using remote or mobile access tools and procedures. The best approach is to have all workers use workforce continuity tools on a regular basis. Although some of the employees displaced during an emergency or incident may not use remote access frequently, they will be more likely to be able to function without assistance in time of crisis if they have been provisioned with WiFi hotspots, 3G connections, or other mobile technologies. To be sure that a contingency plan runs smoothly when needed, companies should periodically check that access software remains operational and that users are adequately trained on how to connect to and use the remote access system wherever they are located.

Based on performing this kind of evaluation, a company can prioritize the rollout of a workforce continuity solution. Going through this exercise gives a company the comfort of knowing that its most critical groups and processes will be given top priority in what may be an otherwise chaotic situation.

Going through this exercise gives a company the comfort of knowing that its most critical groups and processes will be given top priority in what may be an otherwise chaotic situation.

WORKFORCE CONTINUITY CHALLENGES AND OPPORTUNITIES

Challenges

Funding

Ensuring that a workforce can be productive in the face of outages requires some incremental funding to ensure that the proper solutions are in place and "well oiled." Many of these investments involve fixed or recurring hard costs (such as upgrading users to laptops or providing home broadband lines and holding training sessions) that can provide productivity returns on a regular basis as well as when the disaster occurs.

Many of these investments involve fixed or recurring hard costs that can provide productivity returns on a regular basis as well as when the disaster occurs.

For businesses that rely on people to assess systems in order to serve customers, these expenses are as necessary as the expense of installing airbags and seatbelts in automobiles. The business rationale for implementing a solution should be similar to that of buying insurance. Companies should negotiate with vendors to obtain low recurring cost pricing for a system that will help them avoid major business losses when disaster strikes.

Continual Training and Testing

The time a disaster strikes is not the time to find out that a system doesn't scale or users are untrained. The best way to keep a workforce continuity solution current is to require people to use it on a regular basis. In addition, companies have to provide employees with initial and refresher training so that they are comfortable with using the connectivity tools from remote locations and any changes to processes that will occur when a disaster strikes. Companies should plan regular fire drills of the service during which they load up the critical systems and look for bottlenecks as well as determine whether users have the needed tools, connectivity, and knowledge to be effective.

The best way to keep a workforce continuity solution current is to require people to use it on a regular basis.

User Compliance

User compliance is an important part of a workforce continuity strategy's success. It is reliant on users' following the ongoing procedures that ensure that they will be ready to respond when an interruption occurs. This process includes ensuring that all employees have the tools downloaded onto a remote or portable device, whether it is their home desktop or a laptop that they take home with them at night. Companies should make sure that employees take their laptops home every night and that they understand how to use their specific home connectivity. In particular, it is critical to recognize the limitations of working in a worst-case environment, such as dial-up modem, and to factor that into consideration of the applications workers are expected to run or whether they should be instructed to find a faster connection (e.g., WiFi hotspot).

Opportunities

Although companies must overcome some barriers in adopting a workforce continuity solution, they also can realize many benefits.

Creating a Competitive Advantage When Disaster Strikes

Obviously, a major outage can be an opportunity for companies that are better prepared to take market share and enhance their reputation for solid service. This preparedness leads to increased customer loyalty and fewer defections — potentially putting less prepared competitors on the defensive.

Enhancing B2B Selling Proposition and Stickiness

An increasing number of companies request information on business continuity policies from their prospective suppliers as part of the RFP process. Having a solid workforce continuity strategy shows a completeness of vision and builds confidence that companies will provide their customers with reliable service regardless of external events. In effect, such companies become part of their customers' business continuity strategies and thus more entrenched.

Having a solid workforce continuity strategy shows a completeness of vision and builds confidence that companies will provide their customers with reliable service regardless of external events.

Maintaining Workforce Productivity in the Face of Minor Interruptions

Companies can gain advantages on an everyday basis as well. If an event occurs and even a small set of employees aren't able to get into the office, being able to work from a remote location allows them to conduct business as usual. Thus, events that impact employees' whereabouts do not have to impact clients and customers. Companies can continue selling to their customers, as well as servicing and supporting them. In the case of a real disaster, providing employees with remote connectivity to collaborative tools such as email and IM can help managers make sure that all employees are safe and accounted for.

According to recent IDC research, for organizations that have chosen to mobilize an enterprise application, two of the greatest motivators are to realize an improvement in worker productivity and to improve customer service/field service response times (see *Mobilizing the Enterprise 2006: The Long and Winding Road...*, IDC #204717, December 2006). The expansion of existing systems to a broader remote and mobile employee set provides inherent benefits to workforce continuity solutions.

Acquiring and Retaining Talent

Everyday events may keep an employee out of the office; for example, an employee may have a sick child at home or may have an injury that causes short-term immobility. With a remote access solution in place, the employee doesn't need to fall behind on work simply because he or she can't get into the office. Or the employee may be able to get into work but may prefer to work remotely from time to time to avoid lost time commuting or the many distractions that exist in the work environment. Companies may be able to attract new talent and retain their existing workforce by offering a more flexible schedule to their employees. According to IDC research, the mobile office worker and home-based worker segments are expected to demonstrate strong growth — at CAGRs of 5.0% and 4.9%, respectively — from 2004 to 2009 (see *Worldwide Mobile Worker Population 2005–2009 Forecast and Analysis*, IDC #34124, October 2005). In fact, the mobile office worker represents the largest mobile worker segment across the entire worker population. In addition to attracting and keeping talent, companies that can accommodate these types of workers will be better prepared for workforce continuity plans.

Avoiding Financial Trauma

Steep financial losses can be incurred by a company that is not able to conduct business because of a disaster. The old saying that "Time is money" certainly rings true for companies that have experienced downtime. Even a few minutes of system downtime can cost a company hundreds of thousands of dollars. A whole day's worth of downtime may be enough to ruin a company's prospects.

For organizations that have chosen to mobilize an enterprise application, two of the greatest motivators are to realize an improvement in worker productivity and to improve customer service/field service response times.

In addition to attracting and keeping talent, companies that can accommodate mobile-office and home-based workers will be better prepared for workforce continuity plans.

RECOMMENDATIONS

- ☒ Implement both a disaster recovery plan for data and a workforce continuity plan designed to allow all employees to work remotely for a potentially long period of time. Together, these two components can deliver a true business continuity solution. If one component is missing, companies run the risk of losing profits and damaging their reputation.
- ☒ Practice "workforce continuity" on a regular basis by allowing users to work from home regularly. Enabling everyday mobility can serve as valuable practice for times of crisis, especially for employees who do not require remote access. Even if the practice occurs as infrequently as once per quarter, users will know how to get connected and IT will be able to ascertain whether users have access to the proper applications. By following this approach, organizations can ensure that their continuity solutions will actually work under the pressure of real-world incidents.
- ☒ Enable home computers for corporate access. Consider both dial-up and fixed broadband where available. Consider setting up a secure extranet for mission-critical applications and enabling clientless SSL applications so that no additional software is needed. This extranet is an instantly scalable VPN solution for home PC access, and the SSL gateway can perform policy checks. Wireless access — via home WLANs or nearby hotspots — to enable corporate access provides a valuable alternative access method. In addition, wireless WAN access over 2.5G and 3G networks via PC cards (and embedded in popular laptops) is an increasingly viable option.
- ☒ Issue laptops to all employees deemed critical during an outage, regardless of their normal level of mobility or importance. Make it a policy that users take home their laptops every night. Habits take time to develop; thus, employees should be made aware of the policy and the reasoning behind it from day one. Employees who keep their laptops with them at all times not only comply with critical workforce continuity policies but also meet an important requirement of security policies for many organizations. Managers should reiterate this policy often, otherwise employees may not adhere to it.
- ☒ Make sure that remote worker programs allow for rapid scale to the entire employee base after an event occurs. Failure to do so may cause gaps in business processes, resulting in a false sense of security and increased risk. By enabling all employees with the remote worker program, companies can avoid this pitfall.
- ☒ Do not assume that a current remote access strategy can automatically act as a disaster recovery solution. Include additional support and scalability options for both VPN and bandwidth. Consider backups to the VPN solution itself.
- ☒ Continually train and test employees. In the case of disaster or other immobilizing event, there may be neither time nor resources to get processes back before impacting customers. For companies that haven't enabled mobility for all employees, the use of remote or mobile access may be a first-time event for some critical employees.
- ☒ Test the plan frequently. Run occasional tests of the system akin to fire drills for buildings. Make sure that remote users can receive customer support from a third party in case of emergency — when they probably need it the most.

- ☒ Attempt to meet needs through fewer vendors in order to simplify deployment, maintenance, use, and support. Less is more.
- ☒ Ensure access to the workforce continuity solution. It is difficult to predict where users will be located in an emergency situation; some may be at home, in a hotel, at the airport, or somewhere in between. To make sure the solution is as disaster-proof as possible, companies must ensure that employees can access it anytime, anywhere, and over multiple connectivity options including dial-up, fixed broadband, WiFi, WAN, and satellite.
- ☒ Carefully assess the return on investment in workforce continuity. Look for specially priced services that provide a low-cost, hot-standby capability that can instantly scale up in case of emergency.

CONCLUSION

Companies have an ongoing responsibility to their customers, partners, and investors to have a complete and viable business continuity strategy in place. While many businesses have made preparations to protect their data or the operations of their servers in the case of disaster, they also need to have a strategy in place for employees to continue to work through these circumstances. A comprehensive business continuity plan should consist of both a disaster recovery plan for data and a workforce continuity plan for employees.

Drivers for adopting a workforce continuity solution are varied in nature as events both large and small can result in dire consequences to a company. Some drivers are unpredictable and unavoidable, such as natural disasters, epidemics, sickness, political issues, and power outages. Beyond these types of events, however, are many larger business trends that encourage businesses to provide their employees with tools for remote and mobile working. In the case of disaster, the ability to work remotely allows a business to get back up and running with minimal impact to customer relationships and the bottom line. But in times of normalcy, it also allows employees to increase their productivity by being able to work from anywhere they choose.

Businesses need to choose their solution wisely. They need to make sure that the technology is a good fit with their business model and that end users have the necessary resources in place to take advantage of it. Furthermore, companies need to ensure that all end users are thoroughly trained on the system in order to achieve a successful deployment. To ease the IT department's concerns, companies should put security on the list of requirements, but they should also recognize that some security sacrifices may have to be made in the event of a major outage to keep the business running.

Implementing a unified solution can also ease the burden of deployment and support. A viable workforce continuity plan requires multiple access methods and a simplicity of use and management. Combining a patchwork of methods in-house will drain IT resources and probably won't be usable. Such an approach also puts the onus of ensuring reliability, scalability, and solution longevity onto IT when the responsibility could be shared with an expert vendor.

While many businesses have made preparations to protect their data or the operations of their servers in the case of disaster, they also need to have a strategy in place for employees to continue to work through these circumstances.

As the world becomes increasingly flat and reliance on the information worker grows, the need to provide employees with a secure remote working solution that they can use anywhere has been amplified. The benefits of deploying this kind of solution are twofold; it provides an insurance policy in case of disaster and productivity gains for employees who need to work outside the office. Any business that is looking to either develop or retool its existing business continuity plan should employ a workforce continuity solution that includes ample remote access options.

The benefits of deploying this kind of solution are twofold; it provides an insurance policy in case of disaster and productivity gains for employees who need to work outside the office.

VIRTUAL OFFICE SOLUTIONS FROM iPASS

Protracted widespread disasters and temporary business disruptions make every employee a remote worker. iPass helps companies prepare for the unexpected by providing connectivity and device management for the distributed workforce. The iPass Virtual Office service allows all employees to conduct their work from home over fixed broadband lines provided by iPass as well as from remote locations through the iPass global network. Regardless of where employees connect from, connection security and device management are handled, allowing companies to retain management control during a disaster or disruption. iPass provides all of the critical elements for remote connection to a company's network. With iPass Virtual Office, connecting remotely becomes a part of an employee's normal routine and helps enterprises to continually test their workforce continuity preparedness. Customers gain the peace of mind that their employees will be ready to work remotely for an extended period of time, if necessary. To learn more about iPass Virtual Office, go to www.ipass.com.

iPass helps companies prepare for the unexpected by providing connectivity and device management for the distributed workforce.

Copyright Notice

External Publication of IDC Information and Data — Any IDC information that is to be used in advertising, press releases, or promotional materials requires prior written approval from the appropriate IDC Vice President or Country Manager. A draft of the proposed document should accompany any such request. IDC reserves the right to deny approval of external usage for any reason.

Copyright 2007 IDC. Reproduction without written permission is completely forbidden.