access ON DEMAND

WHITE PAPER

Citrix GoToMyPC Corporate

Business Continuity: Managing a Workforce Disruption with Remote Access

Summary

Although no one can say with certainty whether an avian influenza pandemic will occur, business continuity experts and government agencies stress the importance of preparing now. While most companies have focused much planning effort on protecting systems and workplace assets in the event of a loss of power or server failure, many haven't planned how employees will continue working if they are confined at home for extended periods.

This paper describes how you can complete the missing part of your business continuity plans by using remote access to provide employees with access to information and resources during an unexpected disruption. Remote access, when planned properly, can reduce the risks to your business during a workforce disruption.

CITRIX® online

Are You Prepared for a Workforce Disruption?

The scenarios and predictions are dire: Forty percent of the U.S. workforce unable to come into the office because they are ill or taking care of family;[i] up to 2 million deaths in the United States;[ii] a five percent reduction of Gross Domestic Product leading to a recession.[iii]

Whether you consider these estimates to be hype or certainty, experts agree that an avian influenza pandemic is highly likely. Businesses must start preparing now for the potentially devastating effects of such a crisis.

Many businesses have spent time developing plans for business continuity – the capacity to keep essential business functions running in the event of a disruption. However, all too often those plans only focus on protecting systems and infrastructure. Most enterprises feel confident they can manage through events such as power outages and data center outages, yet many are unprepared for a workforce disruption. A recent survey conducted by Citrix® indicates that 42 percent of business technology managers say the weakest link in their business continuity strategy is enabling their workforce to access resources and information remotely in the event of a disruption.[iv]

Even government agencies are not immune to the lack of preparation. Government agencies must be able to continue providing services to citizens, especially during a crisis. Yet only now are government agencies beginning to mobilize. A recent report from the U.S. Government Accountability Office found that only 9 out of 23 federal agencies had plans in place for key staff to work from home during a pandemic.[v] Another Citrix survey of state and local government information technology officials found that just 40 percent of officials said they had disaster recovery and business continuity plans in place to address a potential avian flu pandemic, while 24 percent were unsure if their agencies had such plans.[vi]

Unlike catastrophes such as a hurricane or earthquake, an influenza pandemic will not affect the physical infrastructure of your business. Yet the risks to your business are real nevertheless, because a pandemic can keep your essential employees at home for weeks or even months. There are also liability issues to consider. During a pandemic, ethical and legal concerns will require employers to keep potentially infected employees away from healthy employees. However, businesses must continue running, providing services or products and interacting with customers. The costs of a workforce disruption can be tremendous for vulnerable smaller businesses, but any organization that does not adequately plan for this scenario may face lost customers, lost revenue or even business failure.

Bridging the Gap with Remote Access

A complete business continuity plan outlines how your organization will transfer the performance of services or tasks to an alternative location in a short amount of time during a workforce disruption. The plan should describe how employees will continue working if they are confined at home.

In situations where the office is inaccessible to employees, remote access can provide a safety net that allows workers to remain productive. Whether they are caring for sick family members or are sick themselves, employees can use remote access from home to work for weeks without infecting other employees. According to Gartner Group, IT administrators should include remote access in their response plans to enable large numbers of employees to perform their duties from home for an extended period.[vii]

> *"Have in place completed pandemic/IT response plans that will, at a minimum, enable large numbers of knowledge workers to perform their duties from home for an extended period of time."*
>
> Gartner Research: Prepare Now for a Coming Avian Influenza Pandemic

Today, many companies are offering telecommuting or "telework" options for employees. The technology to enable working from home can often be extended to become a part of a company's business continuity efforts. In fact, one of the most compelling benefits of offering telework technology is for "workplace resilience," the ability to expand work-at-home solutions during episodes of business interruption.[viii]

Remote access can be an effective risk-management tool by enabling your business to decentralize rapidly. The U.S. Department of Homeland Security recommends that organizations identify and prepare alternate operating facilities for the possibility of an avian influenza pandemic, and telecommuting can be a key element to a company's planning.[ix]

> *"Because a pandemic presents essentially simultaneous risk everywhere, the use of alternative operating facilities must be considered in a non-traditional way. Continuity of operations (COOP) planning for pandemic influenza will involve alternatives to staff relocation/co-location such as social distancing in the workplace through telecommuting, or other means."*
>
> National Strategy for Pandemic Influenza Implementation Plan, U.S. Department of Homeland Security,
> Homeland Security Council, May 2006

The Remote-Access Tradeoff

Although many businesses have deployed remote access, many do not want the cost or complexity of extending remote access to every employee. Furthermore, not every employee requires remote access for day-to-day business situations. Yet during a crisis, these same businesses and employees need the flexibility of remote-access technology to keep the business resilient and operational.

While some remote-access solutions, such as VPNs, can be expanded to accommodate higher usage associated with a crisis, there can be significant administrative overhead and cost involved. In addition, IT expertise is necessary to expand licenses and assist users, and that expertise may not be readily available during a business disruption.

Businesses need flexible remote-access solutions that can be activated quickly, require minimal IT effort and require no end-user training. Solutions that can be activated by personnel with limited IT experience can further reduce overhead.

Web-Based Remote Access to the Desktop

Web-based remote-access services can provide an effective alternative or complement to traditional remote-access solutions. In particular, if your business does not have a VPN in place, remote access through a Web-based service can minimize administrative effort, training and cost.

If your business already deploys a VPN or other remote-access method to some users, a Web-based remote-access option provides several benefits. Because a Web-based remote-access solution requires no capital investment and very little IT support, it can help companies expand remote access to fringe users who are not eligible for VPN services due to the high cost and IT effort associated with managing VPN clients and laptops. These solutions can help your organization spend your business continuity budget wisely.

Putting a Plan of Action Together

A complete business continuity plan should include remote access for key employees. Consider the following questions in your plan:

- **Which employees will need to access resources from home?** Prepare a list of the most important knowledge workers in your business. Often contingency plans consider only "mission-critical" employees. Yet these frequently constitute only a small portion of your total staff. Consider the productivity of other staff, such as sales or other "front office" personnel – what if they cannot take orders or work with customers for several weeks? Your HR department may be able to provide better insight into the positions and job tasks for each department. You can then work with the department manager for more detail about the positions.

- **How will these employees work in the event they cannot drive to the office?** If you have remote-access technology in place today, consider how easily it can be expanded to accommodate additional staff. Can employees use it for extended periods? Can it be expanded remotely by IT personnel working from home? What if IT staff is incapacitated – can alternative personnel activate and support the remote-access solution for employees?

- **What resources will employees need to access from home?** Often the resources necessary to conduct business are on the desktop itself, rather than the corporate network. Does the remote-access solution allow access to desktop resources?
- **What advance preparation is required to ensure that employees can get up to speed readily with the remote-access solution?** Does the solution require training or advance setup on the employees' home computers?
- **Are there regulatory compliance considerations for your business or industry, such as the Health Insurance Portability and Accountability Act (HIPAA), the Gramm-Leach-Bliley Act (GLBA) or the Sarbanes-Oxley Act (SOX)?**
- **Are there special considerations for data security in your business?** What are the privacy implications of working on customer data from a remote location?
- **How important is reliability of the remote-access solution?** Does your business face unique situations that mandate highly reliable access to information and data?

GoToMyPC Corporate and the Business Continuity Option

Experts agree that remote access can be the key to a successful business continuity plan, but how does a business manage the trade-offs between enabling every employee with remote access, and the potentially high costs of traditional solutions?

The Citrix® GoToMyPC® Corporate Business Continuity option is an innovative solution for businesses seeking ways to protect against productivity losses during a workforce disruption. The GoToMyPC Corporate Business Continuity option is designed specifically for disruptions that prevent employees from coming in to the workplace by helping you quickly provide employees with a reliable, secure way to work from home or anywhere during a crisis, even for extended periods.

The Business Continuity option is cost-effective and scalable, allowing you to activate GoToMyPC Corporate for every employee when needed, without the up-front expense or complexity of extending your current remote-access deployment for employees who do not typically require remote access. The GoToMyPC Corporate Business Continuity option works like insurance: You install GoToMyPC Corporate on employee PCs, and the accounts remain unused and inactive until a workplace disruption occurs.

More Information

Every business is different. Even if you are not a business continuity manager, Citrix Online can help you ask the right questions about solutions that are right for your business. For more information about GoToMyPC Corporate and the Business Continuity option, contact GoToMyPC Corporate Sales at gotosales@citrixonline.com or call (888) 646-0016.

For more information on GoToMyPC Corporate, please visit corp.gotomypc.com.

NOTES

[i] United States Department of Homeland Security, Homeland Security Council, *National Strategy for Pandemic Influenza Implementation Plan,* May 2006.

[ii] United States Department of Homeland Security, Homeland Security Council, *National Strategy for Pandemic Influenza Implementation Plan,* May 2006.

[iii] United States Congressional Budget Office, *A Potential Influenza Pandemic: Possible Macroeconomic Effects and Policy Issues* (”severe” scenario forecast), December 8, 2005.

[iv] Citrix survey of IT professionals and managers conducted May 2006.

[v] United States Government Accountability Office (GAO), *Continuity of Operations: Selected Agencies Could Improve Planning for Use of Alternate Facilities and Telework during Disruptions,* May 2006.

[vi] Citrix survey of state and local IT officials conducted April 2006.

[vii] Gartner Research, *Prepare Now for a Coming Avian Influenza Pandemic,* December 2005.

[viii] Gartner Research, *Gartner's Telework Maturity Model Defines the Stages Toward Telework Effectiveness,* January 2006.

[ix] United States Department of Homeland Security, Homeland Security Council, *National Strategy for Pandemic Influenza Implementation Plan,* May 2006.

For more information on GoToMyPC Corporate, please visit corp.gotomypc.com

About Citrix® GoToMyPC® Corporate
Citrix® GoToMyPC® Corporate, the #1 remote desktop access solution, is the simplest way to provide secure, encrypted remote access to PC desktops from any Internet-connected computer. A managed subscription service, GoToMyPC Corporate enables remote individuals to use any resources hosted on their desktop just as though they were sitting in front of their PC. Setup takes less than two minutes and security is ensured with an advanced secure communication architecture that uses industry-standard SSL and U.S. government-standard 128-bit Advanced Encryption Standard (AES) encryption, as well as a robust management console that enables IT administrators to customize the security settings.

Citrix Online

A Division of Citrix Systems, Inc.
5385 Hollister Avenue
Santa Barbara, CA 93111 USA

Product Information:
corp.gotomypc.com
www.gotomypc.com/security

Sales Inquiries:
gotosales@citrixonline.com
Phone: (888) 646-0016

Media Inquiries:
pr@citrixonline.com
Phone: (805) 690-2961

www.citrixonline.com