access ON DEMAND

WHITE PAPER

Effective Disaster Recovery:
The Next Best Thing to "Business as Usual"

State and Local Government Edition

Avian Influenza and Other Threats Call for Effective Disaster Recovery Planning

The imminent threat of an Avian Influenza pandemic is recognized by a large majority of state and local governments. Such an outbreak could shut down any government office or facility where even one case of the flu has occurred. To increase social distance, employees could be restricted to their homes or temporary shelters for an indefinite period. At the same time, such a crisis places extra pressure on government agencies to continue providing services to the public and keep informational websites operational to receive citizen inquiries.

Agencies must consider the following dilemmas: How can employees continue working productively if they aren't allowed to enter their office buildings? How can they assist citizens, maintain relationships with teammates and keep key projects moving forward while restricted to their homes? And what is the best way to ensure critical information resources are kept available and up-to-date even when the IT team cannot get into the data center due to quarantine?

If government offices close or employees are quarantined, agencies must be able to provide flexible, secure access to applications, data and people so staff members can continue to interact and assist citizens. Further, if the data center is off-limits, IT administrators need a way to remotely manage systems, including websites, and provide technical support to users. An effective disaster recovery plan must make provisions for data backup and security, flexible access from various devices and connections, and remote collaboration capability.

Citrix Systems, Inc.

Published: June 2006

CITRIX®

Table of Contents

The Challenge: Uninterrupted Access to Government Information and People

In preparing for disasters, whether natural or man-made, today's IT management must minimize or eliminate interruptions in service to citizens, employees and business partners. Access to applications, data and even other people is necessary so that government programs and processes can continue when the workplace closes down (fires, power outages or even a relocation) or employees cannot or should not come into the office (flu pandemic, transit strike or blizzard). Critical aspects of this scenario are: backing up and protecting critical information and applications; providing secure Web access to essential government resources from home or a temporary office; and delivering effective citizen services – the demand for which is likely to be higher in the event of a disaster.

Goals of an effective disaster recovery plan include:

- Providing application and data redundancy through a remote failover center
- Quickly reestablishing employee access to redundant information without waiting to rebuild the network
- Enabling employees to work from alternative locations, including their homes, by connecting to the failover system via the Internet
- Providing a way for employees to remotely access their desktops and conduct meetings and conferences
- Ensuring that employees can continue to provide services and information to citizens – which will become increasingly important and necessary during disasters.

While many government agencies created backup data centers following the 9-11 attacks, the access aspect of disaster recovery is often overlooked in these projects. What good is a redundant IT infrastructure and data backup if employees cannot get access to them – easily, quickly and securely from any location? And what about information stored on office desktops that are off-limits during a disaster? Finally, how can a government agency keep functioning and continue to provide critical citizen services and other "face-to-face interactions," especially over an extended period when travel is impossible or prohibited?

Access Infrastructure Provides the Access Piece of Disaster Recovery

With a disaster recovery plan based on Citrix technology, a government agency can easily handle any of the scenarios that could arise from an Avian Influenza outbreak: quarantined offices, employees restricted to their homes; a data center that is inaccessible; or one that is operating but off-limits to IT.

This paper describes a simulated government agency that is faced with constructing a disaster recovery plan utilizing Citrix access infrastructure solutions. It also explains how an access infrastructure solution can provide simple, secure access to information and other resources that have been duplicated and secured at a failover site. Finally, it discusses solutions from Citrix that deliver a complete access solution for a business continuity plan.

The State Department of Many Services (DMS)

DMS, the State Department of Many Services, is a government agency that provides a large number of critical services to the citizens of the State. Its headquarters and major data center are in Albany, with a second major office and smaller data center in New York City and a third office in Buffalo. Operations are divided between the two data centers although they operate independently. The data centers are responsible for serving the following business functions:

- Access to mission-critical applications for 70,000 departmental users
  - 10,000 in New York City
  - 60,000 throughout the rest of the state
- Access to applications for 20,000 remote and traveling users
- Access to partner applications for business partners

In addition to providing access for all of its departmental users, DMS must give its affiliate agencies in the State and also agencies at local level and commercial partners secure access to data and proprietary applications. DMS uses an SSL VPN to grant access to the specific information and data required by the partners while preventing unwanted access to the agency network.

Within the two data centers, DMS has separate local administrators responsible for maintaining the servers in their respective sites. The administrators are responsible for tasks such as managing applications, restarting servers and monitoring resources at their sites.

Everything was running smoothly for DMS until a legislative audit identified the lack of a documented and tested disaster recovery plan. The auditors explained to DMS that Senate Bill 6195 and the Health Insurance Portability and Accountability Act (HIPAA) require a well-documented and tested disaster recovery plan.

Identifying the Recovery Objectives

DMS immediately began to formulate a disaster recovery plan and concluded that two questions needed to be answered:

Q. *What is the acceptable amount of time the agency's systems can be down? This is commonly referred to as the recovery time objective (RTO).*

As an agency that provides health programs and has 25,000+ children under state purview, DMS cannot afford any downtime for its mission-critical applications. Should these applications fail, citizens' lives could be endangered and some children could be put at risk. To facilitate this requirement, DMS hosts all mission-critical applications on central servers.

DMS also has less-critical applications that reside on individual users' desktop machines. These applications are not essential to DMS's services, so they are not included in disaster recovery planning. Access for remote users does not have the same strict requirements as for the mission-critical applications; therefore DMS decided that remote users and partners can go without access for up to one business day.

After analyzing the user-facing aspects of its programs, DMS focused on tasks that the IT staff performs. DMS needed to determine how long the IT department can go without being able to make changes to their environment in a failure situation. The changes DMS evaluated included tasks such as:

- Deploying new applications
- Adding new users to the environment
- Monitoring the health of the environment
- Maintaining the access infrastructure

Q. *How much data will be lost after recovery? This is defined as the recovery point objective (RPO).*

How much data can DMS afford to lose? After some deliberation, the team decided that DMS cannot afford to lose any data that is relevant to everyday government processes and programs. The data used by the IT staff to manage and monitor their server farms is the only data that is not required to be protected because it is not relevant to sustaining citizen services and is deemed less critical.

Planning for Recovery

With the recovery time objective and recovery point objective identified, DMS was able to plan the details of its recovery. The DMS disaster recovery plan is broken into three distinct categories.

1. **Configuring component redundancy:** Prevents component outage caused by downed servers due to equipment failure such as failed power supplies, network cards, etc. The first aspect is the redundancy of the physical server components.

Listed below are a few recommendations for redundant components.

- Redundant power supplies
- Fault-tolerant RAID (Redundant Array of Independent Disks) setup depending on business requirements (for example: RAID 1, 5, 1+0)
- Fault-tolerant network interface card (NIC) teaming

The second aspect is the redundancy of the services that the physical server provides. After the physical server components are addressed, the focus can shift to creating redundant solutions for the services provided by the servers.

2. **Planning for site failover:** Allows users to be routed from one site to another when a disaster such as fire, flood, hurricane, pandemic, earthquake or power loss occurs.

DMS's initial task was to select a disaster recovery failover site. One of the existing secondary locations could be selected because each has sufficient infrastructure to host a recovery site. The decision would be based solely on the potential disasters that each site faced.

DMS has the benefit of selecting a disaster recovery site from one of its locations. If DMS did not have a suitable existing location, the agency could consider using a third-party data center hosting facility. If a failure occurred, the upstate New York site needs the capacity to support the additional users from New York City and Albany. The reverse is true as well.

For the recovery model, the disaster recovery team had to select between active-passive and active-active. The active-passive model is one in which the disaster recovery data center is in a warm-standby mode until required. All users connect to one of the data centers. The remaining data center is unused until a failure occurs. Active-active describes a disaster recovery environment in which the site designated as the disaster recovery data center is online and functions in conjunction with the primary data center. In this model, users connect locally to the site that has the least latency.

DMS selected the active-active recovery model based on its need to provide improved user experience. The agency requires a full disaster recovery plan that provides access for all department and mobile workers even when one site is offline. Each site is fully redundant and has the capacity to service all users in the entire agency.

Access infrastructure is only one piece of the redundancy and disaster recovery puzzle. However, to have a complete solution, plans must be created for the following infrastructure components:

- Physical network infrastructure (routers, switches, etc.)
- Directory Services (Active Directory, Novell eDirectory, LDAP)
- Network services (DNS, DHCP, etc.)
- Data storage and replication
- Application access and management
- User access points

3. **Defining a component backup plan:** Prevents logical error and user error due to viruses, database corruption, or an administrator accidentally deleting configurations.

The modern computing world has many logical errors that can cause potential downtime. DMS immediately identified threats from viruses, hackers and disgruntled employees. They also understood that logic errors can come in the form of data corruption, such as a database that includes corrupted data. In addition to these logic errors, the possibility exists of a user error causing failure. User errors can take many different forms, such as an administrator who accidentally deletes vital information.

DMS concluded that these logical and user errors are easy to prevent with a well-thought-out plan that includes regularly scheduled backups, along with offsite backup archival.

Providing On-Demand Access

DMS next had to create a plan for providing its employees and partners with flexible access to the resources hosted at the failover data center. In the event of a hurricane or other weather disaster, most employees would evacuate or scatter to other locations. Conversely, if a pandemic forced the DMS offices to shut down, employees would need access from their homes or an alternate office site.

An access infrastructure solution is ideal for disaster recovery scenarios like these because it provides the following:

1. **Rapid access to applications and data using a standard Web browser:** Using the Internet to access agency resources is the most flexible approach during a disaster, because virtually any computer – whether at home, a temporary office or even a public kiosk or terminal – has a Web browser. This allows employees to connect simply and easily from wherever they may be staying during the interruption.

2. **Security over the public Internet:** An access infrastructure solution keeps application processing on the server and delivers virtualized access to users who view and work with the application interface. Therefore, no data is stored on the device. Further, access infrastructure solutions typically provide SSL VPN connectivity to protect the small amount of application data (keystrokes and screen captures) that traverse the network (wired or wireless).

3. **Centralized control over the endpoint:** An access infrastructure solution gives administrators the ability to remotely monitor and control who is accessing information and what actions they can take with the information – such as downloading, saving and printing – based on the user scenario. This is critical during an interruption when users are forced away from their office machines and must connect over untrusted home terminals without government security measures installed.

4. **"Shadowing" capability for remote technical support:** During an interruption, users continue to require support for their computers and applications, but will not have technical resources available in their homes or temporary locations. Through centralized tools such as user shadowing, administrators can remotely view and even take over the user's session to provide support and training needed to keep the employee working productively.

5. **Remote conferencing over the Internet with citizens, colleagues and management:** One of the overlooked aspects of an interruption is the inability to meet with teammates, co-workers, partners and citizens. Remote Web conferencing allows employees to keep in touch, continue collaborating on projects, and connect with partners and citizens to ensure that critical programs and processes are ongoing.

Speeding Disaster Recovery with the Citrix Access Platform

The Citrix Access Platform is a comprehensive information access solution that centralizes applications and information in the data center and enables employees anywhere, using any computer or Web browser, to view and work with them over a network connection.

The Citrix Access Platform provides a consistent, integrated, end-to-end access infrastructure that can accommodate every access variable that is required to seamlessly and securely connect users, devices, and networks to agency resources. It is the broadest portfolio of software solutions for secure, on-demand access to information, applications, and people that is offered by any company in the access infrastructure industry today.

For IT administrators, this solution provides a framework for consolidating information resources for easy data replication, as well as redirection of users to a failover server or data center. For employees, Citrix technology makes it easy to remotely access information resources and conferencing services using any computer equipped with Web browser software. IT staff can also leverage remote access capabilities to manage the IT system from home and provide support via the Web.

The Citrix Access Platform is a vital component of a complete disaster recovery solution. It reduces the impact of natural, accidental, and man-made interruptions by enabling government agencies to recover the comprehensive information infrastructure from the data center to the endpoint user environment quickly, securely, and with minimal negative program impact, and to create a virtual workplace that preserves employees' sense of community and their ability to conduct business as usual.

Citrix enables displaced workers to serve citizens and securely access the agency applications, information and people that they need, from anywhere. Citrix Presentation Server™, the flagship product within the Access Platform, enables applications to be installed, managed, processed and deployed from central servers. Users receive virtualized access to these applications – they view and work with the application interface via the network as if the application were running locally. Citrix Presentation Server supports access on nearly any device or Web browser and network connection, making it ideal for a business continuity situation where users must quickly connect from a home computer or temporary workstation.

Other key products within the Access Platform that support disaster recovery are:

- Citrix Access Gateway™: This universal SSL VPN appliance provides a secure, always-on, single point of access to all applications to protect agency information even when users are connecting over public networks during an interruption.
- Citrix Password Manager™: During an interruption, Password Manager continues to give users the benefit of enterprise single sign-on access. Users do not have to remember each of their application credentials, and with features such as application provisioning, administrators can provide access to specific applications without the need to coordinate credentials with users beforehand.
- Citrix® NetScaler® Application Delivery system: NetScaler devices provide great flexibility in disaster recovery planning with features such as hot failover that allow services to remain up even when one data center goes down. And the application acceleration capability of NetScaler devices keeps performance high even when users are temporarily located farther away from servers.

All Citrix product families are built to work immediately and seamlessly with any IT infrastructure, no matter how distributed and diverse, and with each other. Collectively, Citrix's access products and services deliver business benefits that help agencies to speed disaster recovery. The Citrix Access Platform allows government agencies to:

Quickly Re-Route Employees to Back-up Systems

Citrix Presentation Server provides secure, Web-based access to essential government resources to allow users to work from anywhere using any device, over any network connection. Presentation Server simplifies disaster recovery, assuring access to agency resources by automatically and seamlessly connecting users to the best and/or nearest server group that is available. With Presentation Server, an administrator has the ability to configure zone preference through the use of a policy rule. This policy rule allows the administrator to direct user connections to particular zones in the server farm and to configure failover in the event that a zone is not available. If this policy is configured, the user connection is directed to the server with the highest zone preference and the smallest load.

Provide Employees' Familiar Work Environment at Home

With Citrix access infrastructure solutions, any computer can immediately become an operational workstation. All that is required is a simple Web browser, or the installation of the Citrix client software – available as a free download from the Citrix website – to create a common universal client device. By remotely connecting via a browser or a Citrix client, users regain exactly the same work environment — including their files, their business applications, their office suite, and their interfaces — wherever they are: at home or in temporary business premises. This provides immediate continuity and avoids the need for training.

Stay in Touch with Colleagues and Customers via Web Conferencing

During an extended crisis, with employees scattered and normal routines disrupted, relationships with citizens, colleagues and management can suffer.

Further, maintaining employees' morale is challenging when people are under stress and trying to operate under difficult conditions. Citrix® GoToMeeting™, as a managed Web service, provides online conferencing and collaboration services that allow remote users to continue serving the public, working on team projects and simply keeping in touch.

Protect Confidential Information

When agency staff must suddenly connect from a home computer or perhaps a public terminal, security issues come to the fore. Citrix software protects application data from end to end via an encrypted tunnel. Further, the Citrix Access Gateway with Advanced Access Control enables IT to automate security and compliance measures based on the access context, providing a high degree of control over sensitive information. Citrix® SmartAccess™ technology senses the context of the endpoint and delivers policy-compliant access accordingly. SmartAccess determines who is requesting access, where they are, when access is requested, and how it is requested. If compliant, then and only then will SmartAccess enable access to resources according to policy.

Support Users and the IT System

To remain productive when working remotely, employees need technical support. With Citrix solutions, IT staff can provide remote desktop support over the Web from anywhere. In addition, IT administrators can remotely control and maintain Citrix servers in the event they cannot travel to the data center.

Service Online Requests from Citizens

Agencies that provide self-service or informational websites to citizens may experience a huge increase in hits during a as people seek guidance during a crisis. Citrix NetScaler solutions optimize the performance of Web applications, and can redirect user traffic to a failover data center if needed.

Conclusion

For today's governments, in which access to information is the foundation for survival and the potential for disasters such as flu pandemics are increasing, the need for business continuity planning is more critical than ever. During a crisis, citizens will depend heavily upon government agencies for information, instructions and assistance. To keep agencies operating, maintain citizen services and support employee productivity, it is essential to have in place a technology solution that facilitates fast, simple and secure access to applications, information and people. An access infrastructure solution offers an integrated approach to secure, on-demand access that can allow agencies to create the next best environment to "governance as usual."

The Citrix Access Platform expedites information replication, seamless redirection of users to a failover site, and on-demand access to backup applications and data over the Web. Although government employees may be unable to work in their offices, with the right continuity plan in place, they can still work effectively from home and maintain information resources, such as websites, for the public. With a Citrix solution in place, government agencies can help ensure that employees continue to serve citizens' needs.

Glossary of Terms

ACTIVATION: The implementation of business continuity capabilities, procedures, activities, and plans in response to an emergency or disaster declaration; the execution of the recovery plan.

ACTIVE-ACTIVE SITE: A disaster recovery environment in which the site designated as the disaster recovery data center is online and functions in conjunction with the primary data center.

ACTIVE-PASSIVE SITE: model is one in which the disaster recovery data center is in a warm-standby mode until required.

ALERT: Notification that a potential disaster situation exists or has occurred; direction for recipient to stand by for possible activation of disaster recovery plan.

ALTERNATE SITE: An alternate operating location to be used by business functions when the primary facilities are inaccessible. 1) Another location, computer center or work area designated for recovery. 2) Location, other than the main facility, that can be used to conduct business functions. 3) A location, other than the normal facility, used to process data and/or conduct critical business functions in the event of a disaster.

ALTERNATE WORK AREA: Office recovery environment complete with necessary

office infrastructure (desk, telephone, workstation, and associated hardware, communications, etc.). **SIMILAR TERMS:** Work Space or Alternative work site

BACKUP (Data): A process to copy electronic or paper based data in some form to be available if the original data is lost, destroyed or corrupted.

BUSINESS CONTINUITY: The ability of an agency to ensure continuity of service and support for its customers after an unplanned event. Also, business continuity represents the ability of an agency to maintain viability before, after, and during an event.

BUSINESS IMPACT ANALYSIS (BIA): A process designed to identify critical business functions and workflow, determine the qualitative and quantitative impacts of a disruption, and to prioritize and establish recovery time objectives.

BUSINESS INTERRUPTION: Any event, whether anticipated (i.e., public service strike) or unanticipated (i.e., blackout, Avian Flu) which disrupts the normal course of business operations at an agency location.

CALL TREE: A document that graphically depicts the calling responsibilities and the calling order used to contact agency management, employees, customers, vendors, and other key contacts in the event of an emergency, disaster, or severe outage situation.

COLD SITE: An alternate site that contains physical space and building infrastructure that must be provisioned at time of disaster to support recovery operations. SIMILAR TERMS: Shell Site; Backup Site; Recovery Site; Alternate Site

CONTINUITY OF OPERATIONS PLAN (COOP): A COOP provides guidance on the system restoration for emergencies, disasters, mobilization, and for maintaining a state of readiness to provide the necessary level of information processing support commensurate with the mission requirements/priorities identified by the respective functional proponent. This term traditionally is used by the Federal Government and its supporting agencies to describe activities otherwise known as Disaster Recovery, Business Continuity, Business Resumption, or Contingency Planning.

DATABASE REPLICATION: The partial or full duplication of data from a source database to one or more destination databases. Replication may use any of a number of methodologies including mirroring or shadowing. If performed remotely, it can function as a backup for disasters and other major outages.

DIRECTORY SERVICE: A directory of names, profile information and machine addresses of every user and resource on the network. It is used to manage user accounts and network permissions. When sent a user name, it returns the attributes of that individual, which may include a telephone number as well as an e-mail address.

DISASTER: A sudden, unplanned calamitous event causing great damage or loss as defined or determined by a risk assessment and BIA; 1) Any event that creates an inability on an agencies part to provide critical business functions for some predetermined period of time. 2) In the government environment, any event that creates an inability on any agency's part to provide the critical business functions for some predetermined period of time. 3) The period when agency management decides to divert from normal production responses and exercises its disaster recovery plan. Typically signifies the beginning of a move from a primary to an alternate location.

DISASTER RECOVERY: The ability for an agency to provide business-critical information in the event of a disaster. Disaster recovery consists of activities and processes designed to return the government programs to an acceptable service level after an unplanned event.

DISASTER RECOVERY PLAN: A management-approved document that defines the resources, tasks, and data required to manage the technical recovery effort.

FAULT TOLERANCE: Having a backup system to activate during a primary system failure. An example of fault tolerance with regard to Presentation Server is using database clustering for the data store.

MISSION-CRITICAL APPLICATION: An application, which is essential to the agency's ability to perform necessary business functions. Loss of the mission-critical application would have a negative impact on the government agency, as well as legal or regulatory impacts.

NETWORK SERVICES: Services such as DHCP (Dynamic Host Configuration Protocol) and DNS (Domain Name Service) help simplify network administration. DHCP provides dynamic addressing to keep track of IP addresses rather than requiring an administrator to manage the task. This means that a new computer can be added to a network without manually assigning it a unique IP address. DNS is an Internet service that translates domain names into IP addresses.

PANDEMIC: An outbreak of a disease occurring over a wide geographic area and affecting an exceptionally huge proportion of the population.

OFF-SITE STORAGE: Alternate facility, other than the primary production site, where duplicated vital records and documentation may be stored for use during disaster recovery.

PHYSICAL NETWORK INFRASTRUCTURE: The design of a communications system, which includes the backbones, routers, switches, wireless access points, access methods and protocols used.

RAID: Short for Redundant Array of Independent (or Inexpensive) Disks. A category of disk drives that employ two or more drives in combination for fault tolerance and performance.

NOTICE

The information in this publication is subject to change without notice.

THIS PUBLICATION IS PROVIDED "AS IS" WITHOUT WARRANTIES OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT. CITRIX SYSTEMS, INC. ("CITRIX"), SHALL NOT BE LIABLE FOR TECHNICAL OR EDITORIAL ERRORS OR OMISSIONS CONTAINED HEREIN, NOR FOR DIRECT, INCIDENTAL, CONSEQUENTIAL OR ANY OTHER DAMAGES RESULTING FROM THE FURNISHING, PERFORMANCE, OR USE OF THIS PUBLICATION, EVEN IF CITRIX HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES IN ADVANCE.

CITRIX®

Best Access Experience. Anytime. Anywhere.

About Citrix: Citrix Systems, Inc. (Nasdaq:CTXS) is the global leader and most trusted name in on-demand access. More than 160,000 organizations around the world use the Citrix Access Platform to provide the best possible access experience to any application for any user. Citrix customers include 100% of the Fortune 100 companies and 98% of the Fortune Global 500, all 50 state governments, as well as hundreds of thousands of small businesses and individuals. Citrix has approximately 6,200 channel and alliance partners in more than 100 countries. Citrix annual revenues in 2005 were $909 million. Learn more at www.citrix.com.

0606/PDF

Citrix **Worldwide**

WORLDWIDE HEADQUARTERS

Citrix Systems, Inc.

851 West Cypress Creek Road
Fort Lauderdale, FL 33309 USA
Tel: +1 (800) 393 1888
Tel: +1 (954) 267 3000

EUROPEAN HEADQUARTERS

Citrix Systems International GmbH

Rheinweg 9
8200 Schaffhausen
Switzerland
Tel: +41 (52) 635 7700

ASIA PACIFIC HEADQUARTERS

Citrix Systems Hong Kong Ltd.

Suite 3201, 32nd Floor
One International Finance Centre
1 Harbour View Street
Central
Hong Kong
Tel: +852 2100 5000

CITRIX ONLINE DIVISION

5385 Hollister Avenue
Santa Barbara, CA 93111
Tel: +1 (805) 690 6400

www.citrix.com