

 SearchNetworking.com E-Guide

The Network Professional's Guide to Disaster Recovery

The threat of a pandemic flu outbreak is something that IT departments need to take seriously. To continue operations with staff out sick or working remotely to prevent infection, network managers should be putting plans into place now. A good plan could save your business and offers protection, not only from flu, but from other threats like natural disaster and terrorist attacks. This guide will detail the key steps you need to take today, in order to prepare your organization and network for a potential disaster.

Sponsored By:

TANDBERG

Videoconferencing for Face-to-Face Communication
in times of Crisis



The Network Professional's Guide to Disaster Recovery

Table of Contents

[Network disaster recovery planning needed for avian flu threat](#)

[Top strategies to keep your network running in an emergency](#)

[Unified communications helps enterprises combat bird flu](#)

[The network professional's guide to disaster recovery](#)

[Disaster recovery checklist for the network professional](#)

[Resources from TANDBERG](#)

Network disaster recovery planning needed for avian flu threat

By Andrew R. Hickey, News Writer

August 8, 2006 | SearchNetworking.com

Sept. 11 was a wake-up call, prompting companies worldwide to reevaluate their disaster recovery plans. Hurricane Katrina gave those thoughts another—albeit unwelcome—push. Now, with the potential for an avian flu (also known as bird flu) pandemic—which could be the first true pandemic of the technological age—it's time once again for enterprises to prepare their networks for catastrophe and for the possibility that government edicts could keep 100% of the nation's workforce quarantined at home.

This specter introduces a dilemma: If people can't go to work, how can they stay connected? What can be done to the network to ensure that business can continue?

A pandemic differs from other disaster situations in that the network infrastructure stays intact—it is not destroyed. The trick is to keep everything running smoothly on that infrastructure for a worst-case scenario.

Change the culture

First, however, experts recommend taking a step back. Although changing the network infrastructure now—instead of reacting to the outbreak—is important, experts said the first step in preparing for a pandemic has nothing to do with technology.

"A lot of companies are starting to pre-plan," said Mitch Hershkowitz of Dimension Data, a Long Island, N.Y.-based IT services firm. "But you really have to actually change the culture in order for it to work."

Changing the culture means keeping everyone focused on business continuity. Odds are, not every single piece of the network will be necessary during a disaster. And instead of focusing solely on keeping everything up, enterprises must evaluate what they can do without. "What should stay up and what can we live without?" should be the first two questions enterprises ask themselves, Hershkowitz said.

Ken McGee, a group vice president and research fellow at Gartner Inc., pulled no punches in a recent webcast discussing what to do to prep the network in an avian flu pandemic. Simply put, McGee said, "The likelihood of avian influenza is real. It is a very real concern. It's not something that will go away tomorrow."

Gartner recommends that clients look at their companies' plans to address pandemic needs, McGee said. He estimated that it takes a mere 21 days for a pandemic to spread globally after it is announced. But companies shouldn't just be concerned with their own plans.

McGee suggests immediately obtaining and evaluating written copies of carriers' and service providers' influenza response plans to see where they stand. From there, assess a carrier's remote management strategies, pinpoint its emergency contacts, find out where its backup facility is, and ask about its flu rehearsal schedule and the plan to sustain its own business in a crisis.

Carriers' and service providers' plans make all the difference, McGee said, because without them, the network may not operate.

"We think the pandemic will introduce a very unfavorable effect on the network," McGee said. He cautioned network pros to assume that there will be network outages and travel restrictions, and that people will be working from home and will have their children home from school. That could last 18 months, with millions of people working from home, trying to use residential networks that aren't built to support such capacity.

Backup and collaboration

Companies need to install WAN facilities at employees' homes, according to McGee. If users don't have home broadband, network pros should make sure they get it. If users have broadband, it must be backed up somehow—cable can be backed up with satellite, and satellite can be backed up with fiber. Also, this is the time to start negotiating with Web, audio and videoconferencing providers, McGee said. "Do it now," he said. "Treat it like an insurance policy. Talk to vendors and carriers ... have dry runs; have rehearsals now."

To plan realistically, companies need to assume that 100% of the workforce will not report, so collaboration tools can be crucial. Hershkowitz said that adding collaboration technologies to the network helps keep everyone in touch.

Hershkowitz noted that Web conferencing, whiteboarding, videoconferencing and other collaboration suites need to be in place for times when "a phone call is not enough and an email is not enough."

Yankee Group analyst Zeus Kerravala agreed that collaboration technologies should be put into use now so that users are accustomed to them if the time comes to use them from home for an extended time. He warns that companies should be evaluating collaboration tools anyway, and that bird flu should not be used as an excuse.

Plans defuse multiple threats

Alan Shark, executive director of the Public Technology Institute (PTI) in Washington, D.C., said his company already has several safeguards in place to ensure the network is ready in the event of a pandemic. The plans were not sparked by a potential bird flu outbreak, however. PTI is a mere three blocks from the White House, where threat levels are high. Planning ahead for any kind of threat could also keep PTI operating in a pandemic.

Network disaster recovery planning needed for avian flu threat

PTI has devised a comprehensive plan of action if something prevents staff from physically going to work. PTI has rolled out VoIP, which connects all users with three-digit extensions from anywhere via PC-based softphones that work on a Web-based VPN connection.

PTI has also moved its file server off site and is doing the same with its email server. The network is distributed in such a way that if one part goes down or is overloaded, it shouldn't affect any other parts.

Similarly, the network is set up so that voicemail is sent to email and users can retrieve email via handhelds, meaning that staff would not need to be near an office phone to retrieve messages.

Remote access is key

Robert Whiteley, an analyst with Cambridge, Mass.-based Forrester Research, said the biggest hurdle companies will face in a pandemic is remote access.

Most remote access solutions are built to handle concurrent sessions from 10% of the staff, according to Whiteley. In a pandemic, he said, you need to "flip the ratio on its head" and be able to handle 90% concurrency. He said companies should be looking for a solid SSL VPN that can handle such a monstrous boost in traffic load.

"It's a lot more conceivable to focus on SSL VPNs," he said. "From a technological standpoint, SSL VPNs just make sense."

With SSL VPNs, Whiteley said, users can get onto the VPN through a Web portal on their home computers or PCs that the company sends out. Once logged on, they have the same access they would have in the office on the corporate LAN.

Also, most SSL VPN solutions can scale to meet the needs of many users. For some, one box may be adequate. For others, a daisy-chain of boxes could work to accommodate high loads. Higher capacity costs more money, however.

Along with remote access to reach email and other basic applications, many companies may also want to give users access to VoIP during some sort of disaster, Whiteley said. He suggests making sure that any SSL VPN deployed can handle voice traffic and is bi-directional friendly.

Some vendors have even devised an SSL VPN licensing plan where companies can continue to pay for the 10% usage, Whiteley said. If there were a period of time when usage spiked to 90%, however, the company would be responsible for paying for that spike only, similar to typical overage charges.

To ensure the network isn't overloaded with SSL VPN sessions, a load-balancer could be added, Whiteley said. However, with many SSL VPNs, if one box in the string is filled to capacity, it can automatically bounce incoming sessions to another appliance.

Train and test

Even the most concrete remote access solution could be useless, though, if end users don't know how to use it, according to Yankee Group's Kerravala. He recalled a New York-based company that had an emergency remote access plan in place before the Sept. 11 terrorist attacks, but when the day came, many users hadn't been trained or they had left their remote access instructions in the office.

"There's a fighting chance you might see it coming," he said. "You have to be prepared. Make it part of the process. The more you test, the more the users know. You don't want users having to try to figure things out on the fly."

Kerravala estimated that roughly 80% of pandemic planning is process, while only a minor portion is the tools a company needs to stay connected. He suggests that companies set a mandate under which everyone works remotely one day a month. That will give ample time to test the system and let IT determine where things could go wrong. It also gets users acquainted with new technologies.

"That takes all of the kinks out of the system early on," he said. "You want the user experience remotely to be as close as possible to the user experience in the office."

Most companies already have some sort of remote access plan in place, Kerravala said, but a hurdle is making sure it is of sufficient scale for higher-than-peak usage. Also, different remote access solutions suit different types of workers. SSL VPNs work for those who may need to access only a handful of applications, he said, but an IPsec solution is better for network administrators. The key to determining which remote access solution best suits which group is to understand work flow and work processes.

Still, planning for remote access through VPNs and training workers to use them may be futile if the broadband providers can't scale to meet the needs of specific companies. As a rule of thumb, service providers grossly oversubscribe bandwidth, meaning that if 90% of subscribers tried to use the network at once, the providers couldn't handle the load, and there would be no connectivity.

Most companies should look for a connectivity backup to broadband, Whiteley said, in case a pandemic clogs the pipes and no one can get online. Satellite may not be the best answer because, if VoIP is in use, the latency could be a hindrance. Simple dial-up may be adequate if users only need to dial in to download email, then sign off. Also, a wide-area wireless network could do the trick but would carry a high price tag.

Whiteley said it would be wise to approach Internet service providers to discuss Quality of Service and the amount of broadband you'll need in a pandemic.

"Approach them and say, 'I realize you can't squeeze blood from a stone, but what can you do to guarantee my traffic?'" he said.

Get ready

Whiteley said vendors such as Aventail and Citrix have appliances suitable for planning for a pandemic.

Barry Phillips, senior director of product marketing in Citrix's advanced solutions group, quoted recent research that shows 88% of enterprises are prepared for a power outage, 70% are prepared for a data center outage, and only 13% are prepared for a major disruption in workforce operations. "Most people are just starting to look at pandemic planning," Phillips noted.

Citrix offers four distinct solutions to ensure business continuity in a pandemic, according to Phillips. The Citrix Presentation Server, which works with Citrix Access Gateway, an SSL VPN and Citrix Password Manager, is a single sign-on that virtualizes applications from the server to a user's PC. Citrix GotoMyPC is a remote-access tool through which users can securely connect to their desktop PCs from any computer. Citrix Streaming Server, which also works with the Access Gateway, can download and use any applications to any computer. And Citrix Netscaler is a Web-compression appliance that offers load balancing.

Now really is the time to start looking at the tools that will sustain businesses during a pandemic, according to Gartner's McGee. Waiting until a pandemic is declared will be way too late to get what's needed.

"The hysteria, the concern, the illogical behavior of people will be so vast you will not be able to conduct any planning," McGee said. "We in the information age never had a pandemic before. SARS taught us, and that was a warning shot over the bow...that we were not prepared."

Top strategies to keep your network running in an emergency

By Andrew R. Hickey, News Writer

August 8, 2006 | SearchNetworking.com

Experts agree that now is the time to prep both the network and the company for a potential bird flu pandemic. Here are 14 suggestions from Gartner Inc. on how to proactively take charge of bird flu preparation, instead of reacting to an outbreak:

1. Obtain and evaluate written copies of service provider influenza response plans.
2. Assess service provider strategies for remote management.
3. Identify specific needs not addressed in existing service provider business continuity disaster plans.
4. Seek assurance that externally employed business process experts will be accessible.
5. Recommend that executives identify the most critical employees.
6. Directly oversee the installation of broadband services to the homes of the most critical employees.
7. Install backup broadband services for senior executives.
8. Invest in a backup environment for email traffic.
9. Contract with an external provider for email.
10. Obtain satellite phones for executives, board members and critical staff.
11. Negotiate preferential terms with an audio/videoconferencing provider.
12. Decide whether to lease or buy in-house audio-conferencing systems.
13. Use Web conferencing with clients and suppliers.
14. Assess, recommend and act now.

Unified communications helps enterprises combat bird flu

By Amanda Mitchell, News Editor

August 8, 2006 | SearchNetworking.com

Disaster can strike any day, at any time, whether it's a devastating hurricane like last year's Katrina or an outbreak of the notorious avian flu pandemic that many fear will bring global economies to their knees. During a disaster, the ability to maintain a flexible communication structure among employees, partners, suppliers and customers is the key to survival for organizations large and small.

Unlike hurricanes, earthquakes and other national disasters that occur on a regional level, pandemic flu presents a unique problem because it knows no geographical bounds. Our winged friends automatically make avian flu a global problem. And although it has yet to make the infectious leap between humans, experts fear that human-to-human contagion is inevitable. They therefore say that now is the time for network architects and engineers to make business preparations. IT personnel need to become educated—and to educate others—about the potential crisis, and they must also leverage tools to mitigate communications problems.

"There is a huge burden on communication because so many people conduct day-to-day activities from almost anywhere," said Ken McGee, Gartner vice president and Gartner fellow.

McGee said that—based on recent poll findings—99% of businesses "will not be able to respond to an avian influenza outbreak because of a lack of planning today." This is because almost all business continuity plans today focus on overcoming disruptions to infrastructure and systems. Almost no companies have developed plans for overcoming massive disruptions to the workforce, he said.

Make the workforce ready to brave the storm

Today's IP-based unified communications tools address the workforce issue up front. They lend location-independence to an organization's need for mobile communication and should top the list of technologies to include in a pandemic flu business-continuity plan. When deployed strategically, this set of technologies can play a pivotal role in the jobs of network architects and network engineers who are charged with ensuring that communications—the heart of any business—remain operational 24/7.

People already use a variety of devices to communicate, including wireless phones, PDAs, laptops and smartphones with messaging, instant messaging and text messaging capabilities. In addition, IP phones and SIP-based multimedia tools pull together faces, voices, documents, and presentations into a single virtual, collaborative space. And presence servers, which let callers know whether you're available and which device will reach you most easily, are currently making inroads into corporate communication strategies.

The unified communications concept means breaking down barriers so that people using different modes of communication, different media, and different devices can still communicate with anyone, anywhere, anytime. For example, with its SIP-based architecture, a unified communication platform removes dependence on location, freeing up call centers and IT departments to be reassembled and carried out from a part of the country deemed safe for work. At the same time, cubicle denizens can be instantly transformed into telecommuters by working from home, where they can stay isolated from the deadly virus.

Messaging, collaboration, video, IP phones and presence capabilities are already available from a slew of vendors such as Cisco, Interwise, Mitel, Microsoft, Avaya, Spectralink, Webex and Citrix.

"Companies do need to make plans, whether or not they come to fruition," said Dave Spence, product manager for mobility solutions at Mitel, which makes SIP-based communications products for enterprises and small and medium business. "The simplest form of communication is a phone call. How are we going to guarantee that phone calls coming in will be distributed to the [right] people in your business?"

Spence explained, however, that thanks to IP telephony, an employee can simply take the phone from his desk, stick it in his bag, and then plug into an Ethernet connection at home. "It's the same phone you use every day, so when you get to your home office, features like voicemail and speed-dial ... follow you wherever you go."

One vendor, Interwise, has a take-no-prisoners, redundant approach to unified communications. It makes its client available to everyone in its customer's organization, as well as partners, suppliers and customers. Interwise users typically buy an enterprise-wide license that makes conferencing available to everyone - like email - so should a pandemic arrive, the company is ready to conduct business remotely with every employee no matter where they are. Also, the company is unique in that it provides the option to handle communications on site or seamlessly hand it off to a hosted environment should the need be detected.

"As far as hosted vs. on-site, our customers said they need both. I can't tell you in a pandemic situation if I will be able to get to my own data center or a third-party hosted service, although I could give you scenarios where one is more preferable than the other," said Neil Lieberman, vice president of marketing for Interwise.

For example, Lieberman said, if a company's data center goes down and it can't be maintained remotely, "it's like a ship that's reeling in a storm and everybody runs to one side. That's when everybody runs to a hosted vendor."

"There is going to be more data content going across the wire than ever before," he said. "Are you confident that your hosted vendor will be there when you need it? On the other hand, your on-site solution may be up, and you may be able to get limited bandwidth from your own provider. Users want the best of both worlds, and they want them to work together."

Learning from past disasters

Interwise has living examples of its unified communications technology coming into play in emergencies and saving lives. As a stroke of good luck—or good timing—three months before hurricane Katrina hit, the American Red Cross had purchased a moderate-sized license for Interwise Connect, an unlimited-usage voice, Web and videoconferencing system, for the Red Cross IT training organization. The system had been acquired to help the Red Cross roll out new business and financial software applications to its 800-plus chapters. But with the disastrous fallout from hurricane Katrina, the communications platform took on a more significant role and had to be launched within days.

“The Red Cross usually relies on volunteers, people who aren’t necessarily computer savvy, so they needed a huge number of people to come in to train,” said Peggy Flynn, director of corporate communications. “They couldn’t train down in the area because it was so devastated.”

While the Red Cross is always among the first humanitarian organizations to respond to disaster scenes with supplies of money, food, clothing and other essential items, the organization got its first shot at using a collaboration platform to do its job. In addition to extending support to individuals and families, they were able to qualify and document who received support.

When a disaster occurs, the Red Cross typically will disperse volunteers to the location of the disaster and train them to administer relief using their system. Local Red Cross chapters near the event itself play a big role. Owing to the scope of the Katrina emergency, which wiped out Red Cross centers across the Gulf States, normal procedures to enlist and mobilize the volunteers would not work. In a few short weeks, approximately 1,500 case volunteers had to be fully trained and ready to work before they arrived on site.

Like many vendors able to aid in the Katrina response effort, Interwise – in order to handle more Red Cross users—granted the Red Cross expanded access (at no charge) for Web meetings to be used across the country.

Within days, the American Red Cross began mobilizing individual volunteers at their homes, as well as other chapters that could help outside the disaster zone. The Interwise Connect architecture, which is optimized for minimal bandwidth requirements, enabled the Red Cross to work effectively with volunteers over dial-up and other low-bandwidth connections. And volunteers were able to get online by using the audio device of their choice, including voice-over-the-computer, traditional telephone, cell phone or IP phone.

Interwise is also being deployed by health organizations in many states to support both planning and development for local, state and national response capabilities related to infectious-disease threats. The concept of establishing ways to respond to disease and other biological threats has been active since the mid-1990s, but the events of Sept. 11, the anthrax scares, SARS and other threats have magnified the urgency—and the funding—for public-health emergency preparedness.

The network professional's guide to disaster recovery

By David Davis

July 12, 2006

Implementing and testing a disaster recovery (DR) plan is a huge undertaking. Typically, the number of people involved in developing, documenting and testing a DR plan is proportionate to the number of people at the company and the number of people in the IT group. Unfortunately, there are almost always fewer people than necessary to get the job done.

As a network professional, you need to be prepared to contribute to creating and testing the DR plan, or helping to modify it if one already exists. Non-network people rarely take the network into account when they develop a DR plan. They assume that the network will be there and be functional, even in the event of a catastrophic occurrence.

This makes your job more challenging because the expectations are already set high. To help ease that burden, you first need to make sure you get involved in DR planning. We have developed our network professional's guide to disaster recovery to assist you in this complex task.

The basics of disaster recovery

Before we go into what you, as a network professional, need to know, let's cover some basics of disaster recovery.

First off, there is always confusion between business continuity (BC) and DR. "Business continuity" means that you are just trying to get by until your business infrastructure can be repaired. "Disaster recovery" means that you want to restore the business infrastructure much more quickly. This may mean that larger organizations with critical IT infrastructure have no downtime and are instantaneously providing all business services when a disaster strikes. These terms are often combined into the acronym "BC/DR." Of course, disaster-recovery plans must take into account all business infrastructures, not just IT infrastructure.

A DR plan must be created to plan for the recovery of infrastructure and personnel. Many times, this can be done with a computerized program. For example, my company uses Strohl's LDRPS software to create and maintain our DR plan.

Part of creating that plan will be to determine the criticality of infrastructure and the acceptable amount of downtime. To do this, business impact studies and risk analysis are performed. These studies rank the criticality of infrastructure and staff to help you determine what to recover first or whether there are pieces that do not require recovery.

What can the network professional do to contribute to DR?

In general, the network professional must first be involved in the DR planning phase. The authors of the DR plan need to keep the network in mind when it comes to network applications. (Are there any non-network applications left?)

Network professionals must remind others of the importance of the network in their day-to-day business. This puts me in mind of Cisco's advertising campaign reminding us of "the power of the network."

When it comes to a DR network, obviously, the quickest way to have it available is always to have it up. I have always veered away from DR offerings that say they will "bring up your DR network when you declare an emergency." Instead, I favor a DR network that has the following traits:

- One that is always up and which you can ping any time of the day or night
- One that you can test any time the server/application people can make it happen
- One that has full connectivity to all company locations at the same speed as the production network

Of course, you have to weigh your company's budget against the cost of the ideal DR network. However, the company must take into account the business-impact and risk-analysis studies when considering how much to pay. If all senior managers say that they need email access within one hour of a catastrophe, then the money needs to be found to support the network and server resources to make that happen (or those managers must be told that the money will not be forthcoming).

Disaster recovery checklist for the network professional

By David Davis
August 02, 2006

To assist the network professional in asking the right questions and considering the right topics, we have created the following checklist, broken down into four topical areas: General network considerations, LAN, WAN, and network infrastructure applications.

General network considerations

- When preparing a DR plan, remember to take “partial disasters” into account. For example, if your Internet circuit is down for 48 hours but all other services are functional, what is your plan? Not all disasters include “total destruction of your primary data center.”
- Diagram your current network and identify network devices. What is the criticality of these devices? How do those devices fit into the business-impact studies that determine the criticality of company infrastructure?
- Assuming you have a DR network, how does it differ from your current network? Can it handle the load that will be put on it if a disaster occurs?
- Do you have adequate network documentation for the DR network? When a disaster occurs, everyone will be in a panic. Having proper documentation can be the difference between the success and failure of a disaster recovery.
- How often is your DR plan tested?
- Has proper network resiliency been taken into account for the production network? Think about dual power supplies, redundant network paths and redundant circuits. These network resiliencies may prevent you from having to declare a disaster in the first place.
- What about voice communications? Are you using VoIP?
- Implement a process whereby the DR plan is updated when any new network equipment is implemented or network changes are made. This will keep your DR plan always up to date.
- Make sure you patch and upgrade DR equipment, just as you do other network equipment.
- Don't forget about network security when you have a disaster. No end user will put down “anti-virus software” as a critical need. You don't want to get your DR network up after 24 hours of work only to have it brought down by a virus. You must think about security because users won't.

LAN

- How does the DR LAN network compare with the production network? You don't want to have Catalyst 6500 switches on the production network and Catalyst 2950 switches on the DR network and try to throw the same amount of bandwidth at the DR network. You are setting yourself up for failure.
- Are the LAN network pipes (Ethernet links) the same size?
- Do you have backups of the network configuration files for all devices?

Disaster recovery checklist for the network professional

WAN

- How does the DR WAN network compare with the production network?
- Are the bandwidth and QoS settings the same?
- Have any tests been performed to check the throughput of the DR network?
- Can the routers handle the same amount of throughput as the production routers?
- How do your users get to the DR network in the event of a catastrophe? Routing? DNS?
- Does the DR network have the same security as the primary network? Firewalls? AV? IPS? Internet DMZ?
- Is the same Internet access available on the DR network as on the primary network? What about Internet security add-ons such as content filtering? Proxy servers? Caching servers?
- What would you do if your WAN provider was also affected by the disaster? You could consider having a DR WAN through a different carrier or just put your DR site off of a different POP with your existing carrier.

Network infrastructure applications

- Does your DR plan include a DHCP server?
- DNS Server?
- Does your DR plan include other critical network services such as WINS, FTP and Windows AD?
- Are there network devices that require certain network services to run? For example, some Wyse Winterm devices use DHCP and are then directed to a TFTP server to download their configuration file. You must take into account less-important services such as this because these are often the ones that come back to haunt you.
- What other network infrastructure applications are in use on your network? Have these been taken into account in the DR plan?

Please keep in mind that this is not to be considered a complete IT DR checklist. It relates only to DR and the network. In other words, this checklist is for the network professional who is thinking about how the network and DR are related.

Resources from TANDBERG

TANDBERG

[Benefits of Integrating Videoconferencing into your Business Continuity Plan](#)

A successful business has to think positive—but also be prepared for the worst. The fact is, we are surrounded by threats of crisis every day. The very real possibilities of natural disasters, pandemics, and terrorist attacks require us to be forward-thinking in order to protect our assets.

When emergencies occur, your staff may not be able to reach the office, but your business must continue to operate. Your customers and suppliers will want to know you are still up and running. More than ever, you will need to reach outside experts, share materials, and coordinate your actions quickly. Effective communication is going to be essential.

Videoconferencing is a critical tool to enhance your understanding of a crisis situation and save time when coordinating the **three phases of a business continuity plan**:

1. **Preparation**—Most people think of business continuity technologies as an insurance plan. You hope never to use them, but you need to have them in order to protect your people and your assets. Videoconferencing, however, provides a **return on investment** even if it is never used in a crisis. Training, consulting, product development, equipment repair, and many other activities can be performed remotely over video every day, with the **benefits** of a face-to-face meeting. Moreover, implementing video before a disaster occurs ensures that your system is working smoothly and people are comfortable using the technology—saving crucial time when responding to an emergency.
2. **Response**—Should an emergency happen, video enables you to **visually assess the damage quickly and accurately**. The clarity of face-to-face communication in a very emotional situation allows you to set up a command structure, and collaborate with internal staff, government advisors, and your customers and suppliers.
3. **Recovery**—After a crisis, your staff may not be able to maintain their usual travel schedule or even return to the office for a period of time. Video allows you to **stay connected with remote and home offices** to keep your people working together and continue moving the business forward. You may need to relocate your IT operations to a safe location, and you will require the ability to manage your systems remotely.

TANDBERG's Experience in Disaster Preparedness

TANDBERG has experience in designing videoconferencing solutions for emergency response. We work closely with government agencies such as the U.S. Department of Defense, [EPA's Emergency Response Center](#), [hospitals](#) and [schools](#), and [first responders in local municipalities](#). Our solutions integrate seamlessly with other business continuity technologies, including Web and teleconferencing, PDAs, e-mail, and instant messaging, and 3rd party video units. Video can be implemented securely over IP, ISDN, satellite and 3G mobile networks, to help you respond in a variety of settings. What's more, diagnosis and troubleshooting of the video infrastructure can occur remotely, so that you can manage your systems from anywhere your IT department may be.

First Steps in Choosing a Videoconferencing Solution

Just as your business continuity plan is specific to your organization, videoconferencing is not "one-size-fits-all." You will want to choose the appropriate videoconferencing solution for your network infrastructure, your existing communications tools and your expected applications. Before you pick up the phone to talk to a vendor, take some time to read [TANDBERG's Videoconferencing Guide](#) for a checklist of questions to prepare, and helpful tips on deploying video for maximum productivity.

To learn more about how videoconferencing can address your business continuity concerns, please visit www.tandberg.net.

TANDBERG is a leading global provider of visual communication products and services. The company designs, develops and markets systems and software for video, voice and data. It provides sales, support and value-added services in more than 90 countries.