

# Keep Communications in a Crisis

By Joel A. Pogar

**Reliable communications are important to business operations at any time, but keeping them up and running is especially challenging and crucial when a disaster disrupts normal operations.**

Despite the clear lessons of 9-11 and Hurricane Katrina about the criticality of communications, many organizations remain unprepared to provide key employees with reliable communications and remote access to mission critical resources in a disaster. Often these organizations already have a key element of that infrastructure in place to provide business continuity--in the form of Internet protocol (IP) functionality--they just fail to take advantage of it.

More and more businesses are investing in IP-based communications every day because of the cost savings and the ease of management. Companies consider the business continuity benefits in their decision, but they rarely take the necessary steps to fully leverage IP communications for maintaining business operations during a crisis.

It may first help to define the term. IP communications are those using the Internet; they include voice over IP (VoIP), an alternative telephony function; call center numbers; voice mail and e-mail; and collaborative online environments for virtual meetings. They also include remote access to other corporate network applications through secure connections.

## Case Studies

Let's examine three real-world incidents to see the effects of IP-communications technology on a

company's disaster response capabilities. The first is a company without IP communications; the next two have IP but, as you will see, their experiences vary due to their levels of preparedness going into the crisis. All are actual accounts with which I had experience, but the company names have been withheld and some locations changed to protect client confidentiality.

**No IP in a crisis.** The first business was a major clothing retailer with its principal headquarters in the Florida panhandle. The company had a business continuity/disaster recovery (BC/DR) plan, but it did not have an environment supporting IP communications. Instead, the company relied on a traditional, analog PBX (private branch exchange) and voice-mail system.

Off-site users require a computer, of course. The next question is how they will gain access to the company network. The best means is a VPN, or virtual private network, which establishes a secure "tunnel" from a remote location into the company's main network, preferably an SSL (secure socket layer) VPN.

The cost of hardware, like circuit blades and memory capacity, plus software licensing costs, make VPNs expensive propositions for some firms. Therefore, often only employees designated as key personnel, such as executives, get VPN access. The average worker won't have VPN access due to the cost and overhead of maintaining connectivity.

In the case of the retailer, late summer hurricanes in 2006 caused local flooding, washing out roads and downing power in the area. Amid flooding and power disruptions, the Florida firm, which had a traditional telecommunications infrastructure, became a business in chaos. When I was called in to help re-establish operations, power was unstable

and phones were ringing off the hook.

Making matters worse, help desk support was not available because most employees who would provide it could not access the worksite; those who could were overwhelmed with calls. In addition, the company's designated emergency manager was absent and unreachable; the lack of onsite leadership kept the BC/DR plan from being implemented.

While employees were available at home, and most still had electricity, this situation did not help the company, because staff did not usually work from a remote location, and they either did not have access to the VPN client or did not have the correct VPN configuration. Business was at a complete standstill until an outside vendor could restore operations.

**Continuity in the clutch.** In the second scenario, the business was an online/mail-order sporting goods retailer located in New York. The company was IP-enabled and had a BC/DR plan. An important part of that plan was the IP-Telephony (IPT) system with unified communications. The system provided remote access to the company's information systems for authorized personnel through an SSL VPN (more on this type of setup later).

This system's ability to help with business continuity in a crisis was tested last winter when an unexpected and record setting snowfall of more than 30 inches fell in a 48-hour period; it caused most businesses throughout the city to close for two full days.

During this time, only a small number of employees were able to get to the company's offices. Meanwhile, orders from customers around the country were still coming in, and other operations, such as accounting, were still needed to get bills out and carry out other services.

This situation did not cause a business disruption, however, because the company had established a continuity plan, and had previously purchased access licenses for roughly 3,000 users. Employees were able to access corporate information systems remotely through the SSL VPN with a few mouse clicks. Even if the employees were not traditional VPN users, all they had to do was go to a specific Web site from their home computer or business laptop.

While the company didn't specifically require employees to have home Internet connections or computers, the Web access was there in case it was ever needed. They also designed the environment for a low level of technical sophistication. If an employee could get online, he or she could connect to the corporate network. There was no complex software configuration; setup took just a few minutes.

The company had conducted a capacity planning exercise before implementing its IP-based communications system, so it knew that demand would not exceed available bandwidth in a crisis.

Once logged in to the corporate environment, employees were also able to have calls rerouted to their home phones, cell phones, or to "soft (VoIP) phones" at their discretion. They could access the company's information systems and communicate with other staff, customers, and suppliers all from their home offices.

Loss in productivity was minimal as the BC/DR plan was implemented and communications were rerouted remotely.

**Licensing concerns.** The third example was a major telecom company in the Denver area. In December 2006, a weeklong snowstorm kept employees assigned to its customer service call center from getting to the office. In this instance, the company had a BC/DR plan that presumed workers could operate the call center remotely from their homes via the company's IP connectivity.

The company had already surveyed its roughly 2,200 employees and knew that nearly all had personal computers with broadband Internet service

at home. The company had not, however, addressed the issue of licensing for its remote access software.

When the snowstorm hit, so did the realization that management had forgotten to obtain the extra software licenses that each employee would be required to have. Fortunately, in this case, the company was able to make a phone call and purchase the extra licenses within hours of the time they implemented a work-at-home plan to keep their business operations going.

While the Denver firm's center was not 100 percent staffed, the company was able to use its IP-based PBX and unified communications system to enable employees to remotely answer calls, respond to customers, notify vendors, and keep the business going.

That last-minute convenience, however, came at a cost. VPN licenses purchased for immediate use during a crisis, at about \$9,000 apiece, cost up to twice that of licenses that are purchased ahead of time for contingency use, which are good indefinitely.

### Planning for IP

A resilient IP-communications environment does not need to be complex, but it does take planning. When considering a remote access methodology, SSL VPNs are best.

A traditional, or "client" VPN requires that the end-user's computer have the appropriate software program installed to enable the VPN connection. The software consumes a great deal of memory, requires maintenance, and often creates added IT work.

SSL VPNs instead establish security through a set of "back end" or in-house protocols, removing the software burden from the individual user's computer. Often the user must only download a

single Java applet.

The SSL VPN further eases scalability, making it easier to add new users, especially during a crisis. Depending on the manufacturer of the VPN hardware, many common business applications and protocols are supported for easy operation through the SSL VPN.

(When you access traditional Web mail, or shop online and see a "padlock" icon in your browser's address field, you know that provider is running an SSL application.)

**Assessing functions.** IP connectivity gives employees the potential for remote access, but given the cost of licensing and other factors, it is not practical for a company to plan to provide this remote connectivity for 100 percent of its work force. Thus, a basic question is what functions are critical to the company and must be kept up and running in a disaster?

To answer this question, companies must assess their technology environment before a crisis hits. The key is to identify applications that are mission critical resources and to note which require daily, weekly, and monthly access for business continuity. For example, the HR systems are a necessary part of the business but the company will not cease to exist if an employee record cannot be accessed within 24 hours.

The assessment must be objective. Every person or department in the organization will have personal feelings about which applications are mission critical, and some of those feelings will be strong ones. It is human nature for people to think their environment or application is important to the company. To ensure that the decisions are fact-based, management may want to call in an impartial consultant or appoint a cross-company BC/DR team.

A useful acronym can serve as a guide through this

process, AIDE: analyze, inventory, decide, execute.

*Analyze.* Examine your organization to decide what parts of it must stay operational and for how long. Keep in mind that a crisis situation could last for hours, days, or months. Remember to review and define how long your enterprise could last without a given system.

*Inventory.* Once critical business areas have been identified, inventory the applications they use. Ensure that the application supports IP and can be configured for operation through a company perimeter. Depending on the size and age of your business, you might be surprised to find that some applications still are not using IP, especially in legacy mainframe environments.

Inventory your application licenses as well. Some applications treat "external" users differently from "internal" users based on source IP address. Ensure that you will be compliant with your software licenses if there is a crisis requiring a large number of remote users.

*Decide.* Review the data from the analysis and inventory. Decide what actions need to be taken to guarantee remote access to mission critical resources. Do licenses need to be upgraded? Can your firewalls and perimeter security systems handle the additional load from remote users? Is there a legacy non-IP application that requires an upgrade or replacement? All of these are key decisions to review in formulating a plan.

*Execute.* Move quickly but cautiously in implementing your plan. Set strict deadlines for implementation. Many organizations suffer from "analysis paralysis" and never push ahead to implementation. Or, conversely, a looming crisis (such as a terrorist threat) spurs them into action without a plan. Haphazard implementations can result in application or hardware failures, leaving the company worse off than if it had done nothing.

## Security

While authorized users must have remote access in a crisis, the company must also ensure that security keeps unauthorized users out.

In a crisis, when more workers are going through the firewalls, there will be an extra load on the intrusion detection and intrusion prevention systems as the amount of remote traffic increases. Potential wrongdoers may also be tempted to take advantage of a crisis and gain access to sensitive information.

Strong two-factor authentication systems (something you have, plus something you know) represent the best method for authenticating remote users. The company should have this in place well before any crisis occurs. If the company must rely on a single method of authentication, it is important that systems be monitored carefully.

## Benefits

Once a business gets its IP capability, it needs to know how to exploit its functionality to best serve the company in a crisis. Here are some tips.

Most, if not all, IP-PBX systems allow remote call forwarding. This means that employees can remotely configure their extension to forward all calls to a different phone number, such as a cell phone or home office. However, the system has to be set up and employees trained to take advantage of this feature.

Ironically, this feature is often only made available to employees via the corporate network; it cannot be enabled or accessed outside the company network. This constraint is meant to prevent fraud or abuse. However, it can also prevent use of one of the basic benefits of IP communications--the ability for employees to take business calls at their home, cell phone, hotel, or other designated location.

If your company has invested in VoIP and unified communications, make sure that you are leveraging the technology for all the features it has to offer and that these features can be accessed remotely and securely. One key is to implement measures such as call logs and auditing to ensure that no one can exploit a crisis to commit fraud.

### **Staff Responsibilities**

In addition to setting up the technology and assessing what is mission critical, the company must make sure that employees understand their roles in disaster response. Otherwise, many will think a day away from the office in a crisis is a "snow day" during which they are not expected to work.

Many companies are now developing written HR policies that outline the expectations of the employee during a critical event. Of course, depending on the magnitude of the event, employees may first have to attend to personal family concerns. However, in cases where there is no imminent threat to the employees or their families, it's perfectly acceptable for the company to expect them to work from home to the extent possible.

Details to consider include whether or not the company will reimburse employees for DSL/cable modems, how business use of personal assets will be tracked, and privacy issues regarding personal systems being used for corporate benefit.

### **Legal Considerations**

Even in a crisis, companies must be mindful of their obligations to protect personal data per the plethora of regulations that govern this area. Failure to do so could have serious and costly legal consequences.

As a company assesses which systems are mission critical and might require remote access, it must also weigh the risks with regard to data security. It may decide that granting remote access to some personal data is too risky for compliance reasons. This is just another factor to consider when building and implementing an IP-communications strategy.

The key to surviving a disaster is to prepare in advance and think through the likely impacts: what kinds and degree of demands will be placed on the company's network and IT infrastructure and what steps can be taken in advance to make the infrastructure redundant and resilient enough to handle those demands? If managers wait to figure out these answers when the disaster is imminent, it will be too late.

***Joel A. Pogar, CISSP (Certified Information Systems Security Professional) is director of network solutions at Forsythe Technology, Inc. He has experience in telecommunications, networking, and IT security.***

