



How opportunity connects.

REMOTE DATA CENTERS ARE KEY COMPONENT IN BUSINESS CONTINUITY PLANNING, EXPERT ADVISES

The Challenge:

If you're thinking fire, flood and tornado are the only kinds of disaster you need to be preparing your business for, you just aren't being pessimistic enough. In addition to a rich array of natural disasters, businesses should consider threats from terrorist attacks or chemical spills. And don't forget pandemic viruses, transit strikes or bridge failures.

"There are two kinds of threats to business continuity," says Alec Geist, COO of Pinpoint Network Services in Omaha. "There's the kind that can damage or destroy the workplace such as an earthquake or flood, then there's the kind where network assets are left intact, but employees' access to the worksite is blocked, such as in a flu pandemic."

"In planning for business continuity, if the IT infrastructure sustains damage, considerations for application resiliency, WAN connectivity, data replication and accessibility must be considered," Geist said. "If the event leaves the IT infrastructure in place, then the problem is primarily focused on enabling remote working for the displaced employees

"The ability to continue providing data and voice services to all aspects of the organization should be core to any IT business continuity plan." Geist added, "Whether the workplace is destroyed or employees simply cannot go to the office, having a communications plan for enabling employees to perform their job roles from an alternate work location is essential."



How opportunity connects.

One key to preparing for any kind of business interruption is offsite storage of critical data at a remote data center.

“For many businesses, a tape backup is just inadequate,” Geist said. “Nowadays a lot of companies do all of their network computing from a data center or have mirrored sites duplicating network activity in more than one location.” Geist also said that operating a virtual private network (VPN) from a data center could allow employees network interactivity and access to data via the Internet no matter what happens.

“Companies in Nebraska are especially fortunate because we have one of the most ideal places to locate a data center in the country,” Geist said. In addition to its location near the geographic center of the U.S., Omaha is minimally threatened by most natural disasters and power is plentiful and inexpensive. More importantly, Geist said, Omaha is surrounded by a high capacity “backbone” of fiber optic cable, giving Pinpoint and other data centers in the area easy access to the highest level of Internet connectivity.

The Facts:

In preparing for the IT aspects of business continuity, Geist noted that two-way communication is central before, during and after a disaster, so companies should include emergency preparedness information in newsletters, on the company intranet, and in other internal communications tools. Geist also suggests companies should:

- Assess which staff, data, materials, procedures and equipment are absolutely necessary to keep the business operating.
- Identify suppliers, shippers and other resources you must interact with on an ongoing basis and secure those lines of communications.
- Plan for emergency payroll, expedited financial decision-making and accounting systems to track and document costs in the event of a disaster.



How opportunity connects.

- Provide workers with wallet cards detailing instructions on how to get company information in an emergency. Include telephone numbers or Internet passwords for easy reference.

Summary:

“It’s only good sense to review all your emergency plans annually, not just the IT aspects of business continuity,” Geist said. “As your business changes over time, so do your preparedness needs.”

For more information, contact Pinpoint Network Services at 402-590-1414, or visit them online at www.pnptnetworks.com.