

K rz #w#s#u#s#W#i#r#u#K xuulfdq#h#uhq#h

Focus on people, documents, revenue-producing systems and network capacity

Lucas Mearian

August 26, 2011 ([Computerworld](#))

With [some meteorologists predicting](#) Hurricane Irene could be the worst storm to hit the Northeast in 50 years, IT and business managers need to get some basics about disaster preparedness right.

By the time the storm makes landfall along the mid-Atlantic coast this weekend, forecasters expect it to pack powerful winds in excess of 100mph, posing a variety of "extreme" threats that [include flooding, power outages and damaged water supply systems](#).

It's likely that many workers will not be able to, or may not want to, report for work on Monday due to damage to their homes and concern for family members. That means companies will have to rely on remote employees using VPNs.

"Everyone assumes it'll be all hands on deck, but what's the first thing everyone's worried about? Their family and homes," Bill Peldzus, a vice president at the IT consultancy Glasshouse, said Thursday. "If I was in New York, I would have declared an emergency today."

Peldzus recommends six basic steps for preparedness.


- ε Make sure all company data is backed up off site
- ε Declare an emergency early to get a head start on working out kinks that will inevitably come
- ε Know what's going on with your staff from a professional and personal standpoint
- ε Focus on systems and workflows that pull in revenue
- ε Over-communicate with employees, customers and, for large corporations, stock holders about what you're doing
- ε Be prepared for long-term impacts even if you're not directly hit; power and communications may be out for a while.

"A hurricane is one of the few things companies can prepare for in advance. That affords companies an opportunity they don't typically have when there's a disaster," Peldzus said.

SMBs are the least prepared

While large companies have to be concerned with the details of disaster recovery plans, small- to medium-sized businesses (SMBs) are at higher risk because of their general lack of preparedness.

"My biggest advice to SMBs is to have a very thoughtful conversation with the IT team about the possible scenarios that impact them," said David Chapa, a senior analyst with Enterprise Strategy Group.

Al Berman, executive director of the Disaster 

Recovery Institute International (DRI) in New York City, said that if companies focus on three things -- employee resources, network capacity and critical documents -- they'll come away from the hurricane in pretty good shape.

"One of the things we see when we get lots of water is destruction of documents, including their charter, the checking stuff and all the information they really need to do business," he said. "Even for large companies, make sure you've got all the documents you need -- both electronically and on paper -- out of there."

Berman also said businesses fail to realize that while people worry the Internet will go down during a storm, it's about having enough concurrent VPN sessions so that employees can work remotely.

"Everyone always worries that the Internet is going down. Well, transaction processing uses the least amount of resources on the Internet. While graphics and music uses the most," he said. "It won't be the Internet that fails but the VPN."

Have your head in the cloud

Enterprise Strategy Group on Thursday released [a new report](#) on replication technologies that are available for business continuity and disaster recovery.

Particularly advantageous for SMBs are cloud services, which now offer enterprise-class disaster recovery capabilities at a cost that's affordable. But, don't hog the bandwidth. The more data you want to recover, the more it'll cost you. So store only what you need to get the business running again, and not up to full speed.

When choosing a cloud service provider, make sure you consider where they're located. If they're on your power grid, don't use them.

"A business may think they're pretty well covered because they're replicating data to an offsite [data center](#) miles away, but it may be on same power grid as their office building," Berman said.

One other point to remember is that while a disaster may strike entire regions or coastlines, companies - no matter how large - must learn to react locally.

For example, find out how your municipal [Office of Emergency Management](#), local fire department and electrical utility is planning to react if outages occur.

Companies should have cots, flashlights, food and water on hand for employees who may need to stay in the building during the storm to ensure they can restore systems after it passes.

Chapa said businesses must identify alternative forms of communications for employees, such as text messaging over cellular phones.

Examine your data: What's critical?

Related Blog



Sharon Machlis:
[Hurricane Irene apps, maps and more](#)

"Think of it from an end-user perspective. What are most the most critical data assets. Put them together as part of a solid plan for what it takes to recover," Chapa said.

If your company has a large sales organization, and you predominantly drive business through a call center, then you should have a backup call center in place, along with a list of clients both on paper and in a database.


For SMBs, the question to ask is: What generates revenue? Make sure those systems can be up and functioning in a different location before anything else. "If people are placing orders and you're doing e-commerce, that's your focus. You don't care about HR or payroll," Peldzus said.

Also, consider call trees - or methods of who and how to notify key employees of what's needed after a disaster.

"I had a client in Chicago several years ago who had a call tree, but it was in their facility. During the disaster, they couldn't get into that facility, so they weren't able to get the right people lined up to recover systems," Chapa said.

Last but not least, let the disaster recovery team you've put together do its job. Experts say executives often try to usurp a recovery team's authority after a disaster, which can lead to the failure to recover in a timely manner.

"They go off plan so they don't execute as well as they should," Chapa said. "That's where a lot of companies get wrapped around the axle."

Lucas Mearian covers storage, disaster recovery and business continuity, financial services infrastructure and health care IT for Computerworld. Follow Lucas on Twitter at [@lucasmearian](#) or subscribe to [Lucas's RSS feed](#) . His e-mail address is lmearian@computerworld.com.