Internet Stability in 2009

President, Ministry Business Services, Inc.

Reprinted from *Christian Computing Magazine*

It's only February, and we've already seen more Internet problems this year than I remember in all of 2008! Yet many churches and ministries are deciding to put their most important data on the web… data that, if unavailable, could shut them down. Let's talk about how to protect your ministry from Internet outages and the havoc they can wreak.

2009 Internet Outages

So… what's happened to the Internet so far in 2009 in the U.S.?

- *DDoS Attacks*. Network Solutions "pioneered the service for creating and acquiring specific 'web addresses'". According to their website (where that quote came from), they currently manage more than 7 million domains, 1½ million e-mailboxes, and 350,000 websites. In January 2009 they were hit severely with a DDoS attack.

  A DDoS (Distributed Denial of Service) attack happens when a lot of compromised computers (computers with viruses, trojans, and other malware) all attack a single target at the same time. By flooding it with requests, legitimate users are denied access because it is overwhelmed. That's why so many websites and email systems were unavailable in the third week of January 2009.

- *2009 Ice Storm*. An ice storm hit the U.S. in the last week of January that stretched from Texas, through the Midwest, and up to New England. The ice shut down airports and took out power— and Internet access. Some lost their Internet access because of power outages, while others lost it because the lines over which they connect were down.

- *Google Malware Misfire*. On January 31st someone at Google accidently added a "/" where it didn't belong. The result was erroneous warnings about every site searched, saying "visiting this site may harm your computer!" You might say Google flagged the entire Internet as malware!

- *Turbo Tax Down*. Due to unspecified network issues (possibly a DDoS attack?), Turbo Tax was down February 2nd for most of the business day.

So, What Are You Saying?

First, I am not saying we should avoid using or depending on the Internet in our homes, ministries, or businesses. It is a valuable tool that usually serves us well. But it is not as stable as many think it is. It is vulnerable, and it's vulnerabilities can affect a lot of us all at once.

My concern as an IT guy is that many who are moving their data up to the Internet may not be making the best decision— at this time. Let me get specific.

There are a few categories you could put your data into. Some of it is mission critical, meaning if you can't get to it, you can't do your business and might as well start dusting, filing, or go home and clean out the garage. Some of your data is very important, but rarely mission critical. Other data is convenient, like music downloads or photos… if it's not immediately available, it's not a problem.

I'm concerned about mission critical data. Here are a few possible uncomfortable scenarios:

- It's payday, and your payroll is processed online. Some states have penalties they can levy if payroll is not processed when it's due. Does your vendor protect you from those penalties?
- It's Monday, and your church has its offering and attendance to process. Your church management system (CMS) is only available via the Internet, which is down, so you have to juggle staff and volunteers, hoping they'll be available later in the week; or you come up with a 'Plan B' so you can get your deposit in and then do your processing at a later time. By the way, this also impacts your ability to follow up with visitors.
- Your office phone system connects to the world over the Internet (VoIP) instead of regular phone lines, and because the Internet is down you can't make or receive calls.

These are mission critical systems, and we are dependent on having access to them to get our work done.

So, What's The Solution?

Those who have already moved mission critical data and processes to the Internet need to formalize their backup plan to prepare for those times when the Internet will be down. This is an important piece of the business continuity plan, and thinking it through before the pressure is on— and testing it— can make a huge difference.

Those considering moving mission critical data and processes to the Internet need to ask important questions before pulling the trigger to move forward. And beware of vendors who try to minimize the risk… it *is* real.

- Is the mission critical data or process located in more than one geographical location? Having mirrored sites increases the likelihood that your data and system will be available when you need it.
- Examine the strategy in place that connects your campus to the Internet. If you're heavily dependent on the Internet, make sure you are connected to it through two different trunks and vendors. This is called multihoming. We are in the process of multihoming our offices because we had three outages in the last three years, and our clients need us up and available for them 24•7.

The Internet is not as reliable as it will hopefully be someday. Being strategic about what data and processes we entrust to it can make a big difference in our ability to impact lives for the Kingdom.

Nick Nicholaou is president of MBS, a consulting firm specializing in church and ministry computer networks, operational policies, and CPA services. You can reach Nick via email (nick@mbsinc.com) and may want to check out his firm's website (www.mbsinc.com) and his blog at http://ministry-it.blogspot.com.