

Can The 'Net Support Business Continuity?

Net Forecasts – Peter J. Sevcik
BCR Volume 37, Number 1
January 2007

I have been contacted by readers several times over the past year with the following general question: “My company is developing a business continuity plan in the event of a long-term emergency. The plan states that we will try to continue operations by having our employees work from home via the Internet. Do you think that there is enough bandwidth in the Internet to support this on a wide scale?”

The emergency that they speak of ranges from terrorist attack to a flu pandemic. In all cases, they assume that much of the basic infrastructure will continue to operate but that people will be discouraged from congregating in public places or going to work. Many of the employers, in fact, want to ensure that their essential services continue to function in order for the economy to function.

For example, the Financial Services Sector Coordinating Council for Critical Infrastructure Protection and Homeland Security (FSSCC) says that 99 percent of American financial companies (banks, brokerage firms, trading houses, etc.) have a pandemic flu plan that relies on telecommuting. The FSSCC is depending on federal agencies to help it assess the viability of this work-from-home strategy and make recommendations to solve any problems that are identified. They are basing their assessment primarily on the U.S. National Communications System's (NCS) recently developed modeling capability. The NCS uses this capability to model federal government traffic, and it appears that they are offering to help the FSSCC model some financial traffic as well.

Work-From-Home Requirements

Let us first define what is needed to work from home productively: Good phone service and good broadband Internet service. One may argue that the Internet is much more important than the phone since you can use the Internet for voice, while the phone is a very poor carrier of data.

Yes, you can use a modem over a dial-up line. However, I was recently forced into such a mode of operation while visiting the home of an elderly

family member. I can attest to the ability to get and send email without attachments. But most websites were useless. The continuing growth of Web page size and complexity has made the Web a broadband-only interface.

So the key resources required are broadband access to the Internet, Internet core transit, and circuits from the Internet to your company's datacenters. Each of these service layers must remain operational, provide high availability, and offer sufficient bandwidth for your company's needs.

There are many other aspects of work-from-home that companies must consider. The fact that some users telecommute today is not a sufficient guarantee of business continuity. Even a telecommuting junkie who works every night and accesses services like corporate email every day of the week, will likely not be prepared to be a productive worker for extended periods of time in which he does not go to the office.

Real work-from-home requires a real office setting, including private space, key physical items (documents, manuals, material samples, tools, etc.), dedicated PC, printer, file back-up system, IT tools, communications hub, and even a power generator. Furthermore, the employee must know how to use all this equipment without any help from the IT department.

I know. I work from home exclusively, and I am the IT department for my family. We can get some serious storms blowing in off the mountains that cut power to our neighborhood. I have a system by which I can set up the gas generator, get it running, pull power cables throughout our house, and have essential services on back-up power within 15 minutes. Unless your employees have run such an exercise appropriate to their conditions a few times, you can't be sure that the necessary services will be there when needed.

Asking The Government, “Will Internet Bandwidth Be There?”

The Internet will continue to operate in just about any disaster. The fundamental design principles that made it a survivable network in times of physical attack are still there. For example, the Internet operated remarkably well immediately after the September 11, 2001 attacks on New York and Washington. The question is not will it still work, but rather will there be sufficient bandwidth to support essential services?

I have long been a critic of the federal government’s lack of understanding about Internet bandwidth. I have penned six columns since January 1999 about the extremely poor understanding of bandwidth supply and demand. Many times I have called upon the federal government to gather and publish hard data about Internet capacity--to no avail.

Examples continue to accumulate, demonstrating how valuable such data would be. Just last year (well after the tragedy of 9/11), the Gulf Coast was struck by a series of horrific hurricanes. No one in the federal government was watching or measuring the effects that Hurricane Katrina had on Internet connectivity or bandwidth. One month later, when Hurricane Rita was approaching the same general area, the Federal Communications Commission (FCC) called Internet Perils, a small consulting company in Texas that runs a global Internet connectivity and performance measurement service, to look into what may happen. The only problem: This request arrived just 24 hours before Hurricane Rita made landfall!

There was clearly not enough planning at the FCC. But at least they may now understand the stakes--in the wake of their lack of preparedness, the FCC established the Public Safety and Homeland Security Bureau last September.

In other critical sectors, efforts aren’t that much farther along. The aforementioned FSSCC is relying on the NCS to help the financial community get prepared. Unfortunately, if you look into the charter of the NCS, they are supposed to make sure that telecommunications services continue to operate in support of the federal government. Their primary goal is to keep telephone service (wireline and wireless) operating for first responders, followed by the rest of the federal user community.

That said, the NCS has been quite effective and has made long strides on this important mission for many years. Their work is exhaustive, covering many aspects of communications such as capacity planning, vulnerabilities, infrastructure attacks, cyber attacks, inter-governmental cooperation, emergency communications, interoperability, technology assessment, emergency response activities, etc.

More recently, the NCS has started to model the traffic generated by the federal government on the Internet. It appears that the FSSCC is relying on this modeling capability to help plan for work-at-home in the financial sector.

So it is encouraging that two government agencies are finally looking into Internet capacity and traffic. But businesses that intend to operate during a flu pandemic will likely get very weak guidance from these government agencies, since the agencies are ill prepared to properly study the Internet.

First of all, the NCS and the FCC, as mentioned above, are first and foremost chartered to help the federal government, not corporations. So any help to the FSSCC is a side-line. Second, they are still focused on voice rather than data services. Finally, neither of these government groups is proactively going out to get hard data from the field.

Incidentally, such data-gathering would not be so hard. In the old days of the Bell System, the FCC demanded and got extremely detailed data about voice switching capacity, trunk utilization, time to get a dial tone, call completion rates, call duration rates, etc. The FCC knew very well how healthy the phone network was.

Many of those reporting rules are still in place for the phone network despite the phone company break-up and deregulation. But none of these reporting functions exists for the Internet. If the FCC and NCS just study the work-at-home scenario in computer models, without any hard data on available capacity, then the results will be garbage in and garbage out. It will be full of qualifiers and assumptions.

The Bandwidth Will Not Be There

I propose the following simple analysis of the bandwidth supply-demand problem during a flu pandemic. The U.S. currently relies on non-farm employment of 136 million people. Let us assume that a national flu pandemic forces half these people to stay home. Let us even assume that all of these homebound employed people are working from home using the Internet.

It turns out, of course, that there will be another significant population suddenly at home--students. There are about 65 million elementary and high school students that will also want to use the Internet because they will be bored out of their minds (or may be continuing with some of their studies via distance learning).

So for every work-at-home person, there is a kid who is also using bandwidth. Which one of these groups do you think is a higher consumer of bandwidth? If you had to think about that for more than a second, you obviously don't know any kids.

Of course, many of the employees who would be sent home do not have jobs that lend themselves to telework. If we limit the business-critical traffic to half of what the U.S. Bureau of Labor Statistics calls Professional and Business Service employees (like bankers), then there will only be 8 million people trying to work from home. But in this scenario, *all* the students are still home. So each work-at-home employee must compete for bandwidth with 8 students! The picture does not look good.

The Internet core may well be able to take the higher traffic loads, since there are many redundant networks that typically operate at low utilization. But the warring user populations will certainly cause severe congestion on access networks. Cable and DSL service networks and their uplinks into the Internet core, which are often over-subscribed under normal circumstances, will become extremely overloaded.

How to Overcome the Bandwidth Crisis

Any company that is planning to have their employees work from home should have that employee buy and operate multiple Internet access methods. There will be two keys to getting through: redundancy and priority services.

The first tactic is to purchase broadband service from both the telephone and cable companies if available. It would not be bad to buy even more alternatives. Added redundancy can come from a wireless access service provider, or even a service such as ISDN. Of course, each home will need a multi-WAN router that will continuously monitor the health of the path from the home to the datacenter across the two or even four alternative networks. This will also require sophisticated routing at the datacenter that cooperates with the home routers to switch among networks. The goal is not to put all your traffic on one network at a time but rather to use the alternative networks in parallel, much like a RAID system is used to map files across many hard drives. The redundant networks look like one network to the applications.

Unfortunately, there is no inexpensive router with this kind of sophistication. I suggest that VCs fund start-ups to bring such a product to market as soon as possible.

The second tactic is to purchase differentiated services from any of the carriers that offer them. After many years of not finding a sustainable business strategy for carriers to sell differentiated services, I found this one. An employee of a FSSCC-type company should purchase the premium "gold" service if offered. The employee would not turn on the premium (i.e., packet-marking) service until needed. There may be a small charge from the carrier to have the capability available all the time. The employer should of course run tests to prove that the premium service indeed delivers packets that would otherwise have been dropped during congestion. This gives the work-at-home employee a fighting chance against the kid next door who is playing multi-user games or loading a video over the same DSL or cable access net.

Unfortunately, the carriers that are promoting the idea of differentiated services are planning to sell them to the major content providers as a way to make more money, rather than looking out for critical users during a national emergency. But again, I suggest that the service providers look into this second business model, where they get to make a bit more money during "normal" times (at virtually no cost to themselves), and a great deal more money in the event of an emergency, when the priority service would be activated.

Summary

Companies should use both of these tactics--multiple sources and premium services--in their business continuity plans. The sum of these two approaches will prove much more effective than either tactic alone. Don't wait for the government to figure out if there is a problem and then have them deploy a solution. The best plan is one where you buy and pay for the products and services today in order to be ready for tomorrow. Business continuity is in your hands and only in your hands.

Company Mentioned

Internet Perils (www.internetperils.com)

Peter Sevcik is president of NetForecast and is a leading authority on Internet traffic, performance and technology. Peter has contributed to the design of more than 100 networks, including the Internet, and holds the patent on application response-time prediction. He can be reached at peter@netforecast.com.

NetForecast is an internationally recognized engineering consulting company that analyzes and improves data, voice, and video application performance. We help enterprises align application performance with business needs using a process based on the Apdex standard. NetForecast also advises technology vendors about customer requirements, technology issues, and the business value of application delivery products and services. Visit our library of educational reports and articles about performance engineering.

www.netforecast.com

