



Co-location Basics for Small to Medium Sized Businesses

Copyright © 2004-09, Online Tech Inc.

www.onlinetech.com

Audience

Owners, Chief Executive Officers, Presidents, Chief Financial Officers, Chief Operating Officers of small to medium sized businesses who are dissatisfied with the level of risk to their Internet Servers.

Executive Summary

Many if not most small and medium sized businesses (less than \$500M in annual revenue) rely heavily on the Internet to conduct business. Losing Internet presence means loss of revenue or profits. This mandates highly reliable Internet servers that are protected against local anomalies such as power outages, fire and floods.

Fortunately, data centers built during the boom years are being repurposed into co-location facilities for Internet servers. This result is that small and medium sized businesses can have the same access to first class data centers as the large companies.

As business leaders try to leverage this opportunity to reduce risk they are presented with many detailed choices. This paper summarizes some of the more important considerations.

WHAT IS CO-LOCATION?

Co-location is the practice of putting your equipment, generally Internet Servers, into another's data center. While scary at first thought, the Telecommunication industry has succeeded with co-location for decades. At the core, co-location is the markets response to the enormous capital required to provide high quality, reliable environments for critical communications equipment. By spreading the costs across multiple organizations everyone gets more for less.

Since Internet companies require uptime similar to telecommunications companies the market quickly commercialized co-location for Internet servers. During the late 1990s the telecommunication industry over-built data centers. Many of these data centers have been repurposed to new co-location facilities. The result is that small and medium sized businesses have local access to the same industrial class data centers as the large companies. This local access is extremely valuable.

There are many technical issues involved in designing, building and operating a co-location facility. This paper cover three critical aspects of a co-location facility: the *physical space* in which the server sits; its *connections* for power and Internet connectivity; and the *services* that keep the servers operational.

PHYSICAL ENVIRONMENT

Fire Prevention, Protection and Recovery

Well run data centers prevent fires by avoiding the use of carpet, wood furniture or other combustibles. Tile floors, metal racks, cardboard and paper-free environments all help to avoid a fire.

In the case of fire, the first line of defense is a fire dousing system. Water, Halon and FM200 are the most common. Unfortunately servers and water don't mix well either, so in the case of fire, your servers aren't burnt but their dead due to drowning. Halon is no longer legal as it so drastically reduces oxygen to extinguish the fire that it suffocates anyone who may be in the data center. FM200, on the other hand, removes just enough oxygen to prevent combustion but leaves enough for humans to safely exit the area. Unfortunately, it's extremely expensive and triggers very easily.

The last line of defense is the fire department. Often overlooked, is the proximity to a fire department. If its 15 minutes from fire to firefighting you're server is probably cooked as room temperatures can reach 300 degrees Fahrenheit very quickly.

Recovering from a Fire depends heavily on the level of redundancy and backup. Regular off-site backups and redundant data-centers and redundant server hardware can allow a rapid recovery. Even with this it can take hours to restore from tape and redirect network traffic.

Flood Prevention, Monitoring and Recovery

Air conditioning system can create condensation and water pipes can break. As mentioned earlier servers and water don't mix. To reduce this risk, data centers will install water sensors around AC equipment and other moisture sensors monitors to notify personnel of condensation build-up at hidden but critical locations of the data center.

Static Management

Tile floors of most data centers are anti-static as should be any carpet near the data center.

Access control

Who gets access to the servers, it's power or connectivity? Given that many security breaches occur by insiders it's as important to verify every access as it is to restrict it. Most data centers have key cards or physical keys. While this allows only those with the key card access to the data center, *anyone* with the key card can access the data center. Cameras and biometric screening can be used to manage access while also providing verification. A recent trend is to reduce the need for physical access by providing access to the power outlets, keyboard and screens one gets while at the server securely through the internet.

CONNECTIONS –ELECTRICITY, INTERNET CONNECTIVITY

Your server is connected to wires that supply power and connectivity. These resources are much more critical to Internet servers than typical office equipment. At the same time, their reliability is being challenged by the exponential growth rates and external human elements such as terrorism. A number of pieces of equipment are involved in managing power for a data center. It's best if that power equipment is in a room separate from the co-location servers.

Power Availability

Power, one of the oldest utilities turns out to be one of the most challenging resources to obtain in the appropriate level of reliability and quality for Internet servers. There are limits to how much of it you can bring into the facility, how much you can backup with battery, how much you can clean and how much you can backup with generator.

Power Quality - Spikes

It begins with supply – the quality and reliability of the power coming from the provider (e.g. Detroit Edison here in Michigan) has too many anomalies to properly supply an Internet server hour after hour. That power must be “cleaned” by removing spikes and steadying the flow. The cleansing is done directly from the power feed within the data center.

Short-term Power Loss - Brownouts

Next it has to be stored in batteries for use in the case of outage. Imagine what happens when you unplug your laptop from the wall – the battery seamlessly takes over. Servers in a co-location facility must have similar battery backup to assure their operation is not interrupted during short-term power outages or brownouts.

Long Term Power Loss – Blackouts

For power outages that outlast the batteries a data center uses a generator. There are two types of fuel sources for generators: natural gas by pipeline or diesel from a fixed tank. Natural gas provides energy for the generator until the natural gas company can no longer provide natural gas. In a geological catastrophic event natural gas supply could be interrupted. Diesel tanks can provide fuel to the generator, but like the battery has a limited supply. When the diesel fuel runs out the Internet servers go down.

Connectivity and Internet Bandwidth

Connectivity and bandwidth are two different things. A telecommunication provider (e.g. SBC) provides a dedicated line to an Internet Provider for *connectivity*. The Internet Provider (e.g. Verio) then sells you bandwidth with which you can send and receive Internet traffic. You will pay for the amount of traffic you use based on a formula driven by time and the peaks and valleys of your usage – this is called buying *bandwidth*.

It's important to have multiple connections into the Internet, to different Internet providers. As well, you need to have the ability to seamlessly switch from one connection and Internet Provider to another with minimal disruption to the Internet Server. This leads one to examine the data centers internal network

Internal Network

As the connectivity comes into the facility, it is shared amongst many Internet Servers, each requiring their own secure, private access to the Internet. This hardware, a collection of switches and routers, are architect in a way that Internet Servers can only share appropriate traffic and that one can fail with no to minimal impact on the Internet Servers. Ideally, there are redundant edge routers, switches and internal routers cross-connected so as to always be available to service any server.

Physical Access

There are many aspects to physical access to servers in a co-location facility. First is access to the building housing the data center. Once in the building, one needs to control access to the data center room itself. Within the data center there could be multiple co-location customers. Each should have secure, private space for their servers. Often overlooked is access to power and connectivity feeds. Can someone cut the power going into your cabinet? Ideally these are run through conduits to every rack from separate rooms housing the power sources and the internal network equipment. Customers should only have sole access to the servers.

Virtual Access

A more recent development is to use special power strips and hardware attached to the Internet Server to allow your secure internet access to the power outlet running your servers and to the keyboard and monitor. These features allow you to shut down your servers, reboot them and perform system administration without having to have physical access. This can reduce the need for physical access.

ADDITIONAL SERVICES

When you co-locate your server in another data center, additional services may be critical to a successful, low-risk experience.

Offsite Backup

Many servers these days have tens of Gigabytes of information that would need to be restored to recover from a failure. For the best reliability, the data on this server should be backed up nightly and taken off-site. But given the volume of data it's not feasible to backup your servers through the Internet. Backup services offered by the co-location facility can address this problem providing you off-site tape based backup.

Onsite Hands and Eye

In the case of hardware failure, someone will have to visit your server at the data center to replace the defective components. Ideally, your co-location provider can reliably perform those functions avoiding a trip by your technical staff. As well, some facilities allow your staff access to a locked closet with spare parts for your servers.

Private Partial Racks

How much space do you need to store your servers? If it's less than a rack, you may be able to purchase $\frac{1}{2}$ or even $\frac{1}{4}$ of a rack. Sometimes this rack is shared by you and two or more other co-location customers. Obviously this can be a security risk. Ideally, you can purchase partial, private and secure racks.