

NotesOn: Risk Management - Datacenter Assessment - Part I

Introduction (v1.2):

This post provides a high level overview of the best practices surrounding the selection of your Primary (or Production) and/or Alternate (or Disaster Recovery) Datacenters. The “excruciating” assessment details will be discussed in Part II but for them to make sense it is best to understand the framework in which they fit. Finally, while this is not an exhaustive dissertation on the subject it does address most if not all of the fundamentals, and with them under your belt you can more wisely determine your best solution.

The information herein is based on extensive experience and research, garnered over quite a few years while designing and building IT systems from top to bottom and while safely housing those systems to ensure they were available when needed.

Introduction (V1.2):	1
Background:	1
Datacenter Best Practices:	2
Summary:	6

Background:

Over the years I have both helped build out, and seen built out, quite a number of datacenters, also others renovated and upgraded, and still others that should have been upgraded but were left jammed to over-capacity. I have spoken to and learned from true and so-called experts, all verbally touting their “best of breed” solutions – some of which were, and some of which were no breed at all. In all of that time, however, I never did find a single reference source that laid out what one needed to look for, and at, while deciding how to solve both current and future data storage and protection needs.

Which, by the way, is the whole and entire point of a datacenter, to adequately store and protect your data (and, oh yes, the equipment it runs on).

Many of the small-cap(italization) business folks I’ve worked with over the years grew with their “datacenters” starting out in a closet (some with air conditioning and some without) or in a converted office space on one of the floors in their building – you can still, to this day, find critical systems stuffed away in closets (or worse sitting on top of someone’s desk). While that approach mostly worked during their start-up days, it was, of course, terribly unworkable as a long term solution.

As the need for computer processing grew the mid- to large-cap companies I was associated with took over one or more entire floors of their building (or one very close by), filling the space with raised floors, tons of “big iron” and massive amounts of air conditioning. The cost of the square footage of the downtown floor space burned up by these computer equipment centers was staggering.

Of special note is that in the “early days” *everything* was very local. The datacenters that we know today did not exist, with a very few data processing (usually payroll) companies being the exceptions. The problem with local is that it was, well, local. If anything happened to the office it also happened to the datacenter ...

As technologies improved, particularly the increase in bandwidth of phone/communication lines [[Trunk lines \(T1-T4\)](#) and the [Optical Carrier \(OC-\)](#) series], companies began to move their computer equipment centers out of high-density high-cost city cores into more remote locations. The new sites were still expensive just not as, so in the long run it was an ROI worth obtaining. Then a few of these more distant centers were “lost” due to storms and other “issues” and the impact on company survival was so severe IT folks began looking beyond ‘less expensive’.

No, it has not been easy. The road to getting to where we are now, which is not an end but an “in progress”, was a long and painful process with a good deal of technical “wing it” involved.

I distinctly recall tracking down and buying my first UPS’s (uninterruptable power supplies, i.e. battery backup and power filtering units) because both power outages (and brown outs) and industrially generated noise on the power lines were coming into the building and wreaking havoc on my equipment and, of course, all of the data. I clearly recollect running miles of cable through supposedly isolated “safe” areas only to discover that a microwave tower was shooting beams over the top of the building and interfering with, scrambling, our data signals; requiring re-running specially shielded cables. I remember having to recover system after system because the “air conditioning” in the computer center was insufficient to keep up with the rising heat load as more and more gear was installed. These are just a few examples from a whole laundry list of “events” that marked my, and others’, experiences with keeping IT equipment up and running. We won’t even get into the number of times customers saw no need to do backups (let alone take tapes off site) ... until it was too late.

Bringing IT equipment “out of the local closet” and upgrading it to more resilient and expensive “state of the art” solutions was an often painful, error marked, process in the “early days”. And it often remains so today. In part because the fundamentals behind the “care and feeding” of datacenters is not widely known.

Datacenter Best Practices:

1. Having all of your data, IT equipment and backups centered in one location is a bad idea. No datacenter is “bullet proof” against every and all potential emergencies, thus there is little or no resiliency, little or no protection against an long outage or outright loss in the event a local or regional disaster occurs. Relying on a single location is akin to playing “russian roulette” using a revolver with at least two (if not three) of the six chambers filled with live ammunition. Murphy’s Law strongly suggests that sooner than later you will lose your IT equipment and data. When you lose all of your data you are most likely out of business.

One of the most valuable and critical tasks in your decision tree when it comes to datacenters, what should require a significant investment in time and energy is where you locate *them*. As in plural. We will discuss this in detail in Part II, but the long and short of it is ... do not short change this step and, please, use an extra measure of common sense.

Real Life: one company had two datacenters but they both were well within the absolute, bare bones minimum separation limit of 20 miles. The risks of close-proximity should be obvious.

Real Life: a company had no secondary datacenter. All their eggs were in one basket. It cost them their business.

Real Life: the company's off-site tape storage vault was almost directly across the street from their primary datacenter. They had overlooked checking the address of the vendor.

2. All data of importance should be backed up to a separate location at least a reasonable and rational distance away from the primary data creation/usage location. Possible solutions include:
 - a. Sending backup tapes to a remote "off site" location
 - b. Copying data (and supporting software) to approximately equivalent computer equipment at a remote "off site" location in such manner that the system(s) can be brought up in "short order", with "short order" being defined as what is acceptable for that system and its data
 - c. All of the above (the preferred answer)

Real Life: the owner of the company had absolute confidence in his hardware and thus did not concern himself with daily backups. When his back room "datacenter" failed, he lost everything. Customer lists, vendor lists, parts lists, A/P records, A/R records, G/L records, etc. all had to be reconstructed.

Real Life: almost uncounted numbers of companies lost all of their data during and after Hurricane Katrina. Needless to say, but I will anyway, they went out of business.

3. There are many honest salesmen and women but, nevertheless, you should still do your own assessment /inspection of your existing, or future, datacenter. We will address this too in great detail in Part II of this series but, for now, know that the following categories must be examined/audited in an unbiased manner:
 - a. Customer Satisfaction
 - b. Power
 - c. Cooling/Air Conditioning
 - d. Fire Detection/Prevention
 - e. Security/Datacenter Monitoring
 - f. Location, Location, Location
 - g. Expansion Room / Over-utilization

- h. Network Feeds
 - i. Technical Support
 - j. Disaster Recovery/Business Continuity Planning & Plans
4. Inspect/audit your datacenter on a regular basis. Not just before move in. Look for on-going maintenance of and continuous improvement in the above inspection areas. As one example: look for “over booking”. There may have been expansion room when you moved in but more than one datacenter has been quietly “over-max’d” to the point where what used to be adequate-or-better is no longer. When this occurs, and it is more often than you suspect, the facility no longer has the resiliency to protect your systems and your data. Imagine putting 30 or more amps of lights and electronic components on a 20 amp circuit. Sooner than later ...

Real Life: the datacenter the customer was in was max’d out, it was at 100% utilization on power, cooling and space. The datacenter had no margin of safety, at all. Any slightest failure of the datacenter’s (internal or external) infrastructure and the customer would lose many of its critical systems, a number of which existed only and entirely in that datacenter.

Hint: if the provider refuses to allow you, an honest legitimate customer, to inspect the datacenter in its entirety suspect over-booking or other egregious failings and start looking for another provider. Using security as an excuse to prevent you from touring the facility is a common one.

Virtually all datacenters house their customers’ systems in secure cages that are *not* accessible to anyone but those specifically authorized entry. Thus. There is no earthly reason why you, as a loyal, or future loyal customer should not be provided escorted access to the entire building – from the Network Operations Center, to the Generators and UPS/Switch Rooms, to the A/C units/towers, to a walk-through of each and every floor. An experienced eye should quickly be able to gauge whether the sales folks have oversold their facility. It doesn’t happen routinely but it does happen.

5. Ensure critical datacenter systems are tested regularly. Do not ignore this one at your own peril.

Real Life: the customer had been using the datacenter for years. They finally decided to test some of the internal emergency gear. When they intentionally tripped the Automatic Transfer Switches to fail over from city to generator supplied power the switches did a complete melt-down and the entire datacenter went down, hard – neither city nor emergency generator power was able to get beyond the switches, plus the UPS (battery) backups were insufficient to keep anything running. The good news was that some of their critical systems failed over to an alternate datacenter. The bad news was that only a few of their critical systems were able to fail over to their alternate datacenter. The good news was that they did find the problem and fixed it before the datacenter went down in the midst of a storm or other disaster. The bad news was that it was a very, very expensive lesson learned.

6. If at all possible have a small team of your own people at the datacenter(s).

Real Life: almost as soon as the contract was signed the “first string” support technicians promised to the customer were replaced by “second string” (i.e. less qualified and trained) people. The vendor’s excuse, when the customer complained, was that they had other higher priorities to attend to and they needed their best people on those *other* accounts.

Real Life: in another case even the “second stringers” were replaced by wet-behind-the-ears “third string” neophytes. As out-sourced service levels became intolerable I recommended to the customer that they hire/re-hire their own people to take over all but the most mundane (take Tape A out of the slot and put Tape B in the slot) tasks at the datacenter.

It may seem a “tad bit” cynical to say so, but the truth is that no one is going to look after your equipment and data like your own dedicated employees. This does not mean that all for-profit datacenter personnel are “bad” or “two faced” or “dishonest”, that would not be at all true, but:

- Any number of scenarios present themselves to vendors which makes it terribly tempting to “borrow” technicians who were promised elsewhere. One can understand true emergency situations when another customer’s systems go down, but with some vendors any excuse becomes “good enough” if you let them get away with it.
- As I’ve noted in other posts, there is a dark-side-of- human-nature rule that I operate by whenever appropriate, and keep in the back of my mind always: for too many vendors their first priority is, and will always be, the survival of their company, the protection of their jobs ... not your company and your jobs. This philosophy is, to be sure, 100% backwards: providing good-to-impeccable service at a fair price is the best guarantee of *having* a future. And, in this day and age, that is most often *best* guaranteed by your company’s own employees. [In this age of free-wheeling out-sourcing, and in particular off-shoring, that may be a hard fact to swallow but I’ve seen it prove itself time and time and time again.]

Stated in a different way, there are quite a number of honest datacenter providers in the marketplace who do, for the most part, provide good quality service. However. There are also (and this is the reason I’ve included ‘6.’ in this best practices list) more than a few who live and breathe the above “dark side” rule.

Real Life: It is a violation of this site’s [Rules Of The Road](#) to mention company names so suffice it to say there is one well known outfit whom I will never ever recommend to anyone under any circumstances. In the heat of seeking more sales (their greatest strength), they employ the “dark side” rule constantly. Think you’re *their* number one priority? And always will be? Wait until the ink is dry and then think again.

Moral: write your Service Level Agreements very carefully; including appropriate, hard hitting, penalty

clauses aimed at defeating “first string” substitutions.

7. To help you avoid some potential divergences from these best practices, please do not lock yourself into long term contracts, at least not in the beginning. Consider that first contract a “proof of concept”. Leave yourself an ‘out’. Leave yourself a back door so if you find that the “dark side” rule, from ‘6.’ above comes into play you can, and your equipment and data can, get out of the contract and out of the datacenter.

Recommendation: begin with no more than a 2 year contract and then, based on lessons learned and actual Service Levels obtained, decide, fairly, to extend the original contract. No organization, yours or anyone else’s is perfect. But. If you run into constant service issues and too many “we’ll make it better” fix-it programs or excuses from the vendor ... move on. Despite the additional costs, move on.

Summary:

The above Real Life examples are but a few that I could have raised (these were simply the ones that came to mind at the time I needed them). And the above Best Practices overviews are based on hard learned lessons.

None of them are impractical, pie-in-the-sky guidelines dreamt up in some dark and dank office late at night just to stir up trouble between you and your (now or future) datacenter vendor. And please do not take them so. We will get into the greater detail on how to avoid departing from these best practices in Part II but the data above is, by itself, an honest to goodness, rock bottom starting point to ensure that your relationship with your datacenter(s) is and remains both good and long term.

Hope this helps,

DP Harshman

PDF Link