

5 NEGLECTED DATA CENTER RISKS EVERY EXECUTIVE MUST UNDERSTAND

Table of Contents



Section	Page
1. Introduction	3
2. People Risk	3
3. Design Risk	4
4. Operations Risk	5
5. Contract Risk	6
6. Financial Risk	6-7

CBRE © 2016 All Rights Reserved. All information included in this proposal pertaining to CBRE—including but not limited to its operations, employees, technology and clients—are proprietary and confidential, and are supplied with the understanding that they will be held in confidence and not disclosed to third parties without the prior written consent of CBRE. This letter/proposal is intended solely as a preliminary expression of general intentions and is to be used for discussion purposes only. The parties intend that neither shall have any contractual obligations to the other with respect to the matters referred herein unless and until a definitive agreement has been fully executed and delivered by the parties. The parties agree that this letter/proposal is not intended to create any agreement or obligation by either party to negotiate a definitive lease/purchase and sale agreement and imposes no duty whatsoever on either party to continue negotiations, including without limitation any obligation to negotiate in good faith or in any way other than at arm’s length. Prior to delivery of a definitive executed agreement, and without any liability to the other party, either party may (1) propose different terms from those summarized herein, (2) enter into negotiations with other parties and/or (3) unilaterally terminate all negotiations with the other party hereto. CBRE and the CBRE logo are service marks of CBRE, Inc. and/or its affiliated or related companies in the United States and other countries. All other marks displayed on this document are the property of their respective owners.

1. Introduction

The data center industry has matured significantly since the late 90's. Third-party providers have become more experienced at building and operating data centers than enterprises could have ever hoped to be. There are also more providers than were available even five years ago. While increased competition is advantageous for the buyer, more options make 'choosing' more confusing and complicated.

DON'T FORGET THE PRIMARY ROLE OF THE DATA CENTER

Whether you are G500 Financial or SMB, the top priority is most often **PROTECTION**, and while most data centers share a common objective, most people and providers are not **'objective'**. Being too parsimonious or quick in your decision may yield some unintended and potentially disastrous consequences for your corporation.

As an executive, it is your duty to understand and mitigate the risks to the technology enabling your business. That often starts at the data center.

2. People Risk

People still pose the greatest risk to data centers. A friend of mine once said, *"In a multi-tenant environment, you're only as safe as your least responsible neighbor."* As it turns out, we humans are not rational, logical, or reliable in most cases.

Research indicates that the majority of preventable incidents relate to human error and process failure.

As a general rule of thumb, the fewer people (internal or external) within regular proximity to your IT equipment and the corresponding mission critical infrastructure, the better. One particularly notable exception is the exceptionally well-trained and experienced technical operations team. In the event of an incident related to a complex system (i.e., data center), their ability to adapt to the situation could save the day.

3. Design Risk

Data center electrical and mechanical designs vary significantly in many cases. The newest design derivatives promote a more efficient utilization of capital and a lower price, but can come with trade-offs. Some solutions even allow for the resale of YOUR redundant UPS capacity. (It only becomes yours if you need it and if nothing else breaks when you need it.)

Most customers only utilize 50% to 70% of their leased capacity at any given time.

Consequently, some providers employ oversubscription of UPS capacity to maximize utilization and profits. Under normal operating conditions it may work just fine however, when a disaster strikes you will be competing with your neighbors for that last bit of capacity and may find yourself out of luck. It is comparable to overbooking airline tickets, except that travel vouchers don't fix the problem in a time-sensitive emergency.

Understand to what components redundancy applies. While SLA's are commonly called out in your contract; resiliency may not be. What specific critical elements (electrical, mechanical, fiber entrances, generators, etc.) are redundant and at what level? If your provider has a problem disclosing this, be cautious. Request proof of design, construction, AND commissioning certifications.

Choose the Right Design(s) for You

Choose design(s) that match the criticality of your infrastructure. In many situations, it makes sense to support different parts of your environment with various design redundancies, locations, and even providers. At a minimum, select a concurrently maintainable or fault tolerant design for mission-critical business applications, and protect non-critical IT infrastructure with lower resiliencies to achieve any desired cost savings.

Inaccurate capacity forecasting is the #1 reason enterprise customers over commit, and most do so by 100% or more!

Build, buy or lease the 'right' amount of capacity. Too little is risky (sans the appropriate expansion rights); too much is costly (sans the rarest of exit options). Double and triple check your IT organization's calculations and assumptions! The majority of IT organizations stretch just to maintain the day to day demands of the business. Others fail to plan sufficiently for innovations that are enabling more efficient AND more powerful IT infrastructure. In other words, by the time you move into your facility, your new equipment consumes less space, power and cooling than you planned for. The capacity planning conundrum is even further exacerbated as cloud offerings become more acceptable and mainstream to enterprises who once discounted them a too risky.

4. Operations Risk

In 2014, 25% of Uptime Institute survey respondents indicated they experienced a business impacting outage in their colocation facility.

HOW MANY BUSINESS IMPACTING OUTAGES AT YOUR PRODUCTION DATA CENTER IN PAST 12 MONTHS?

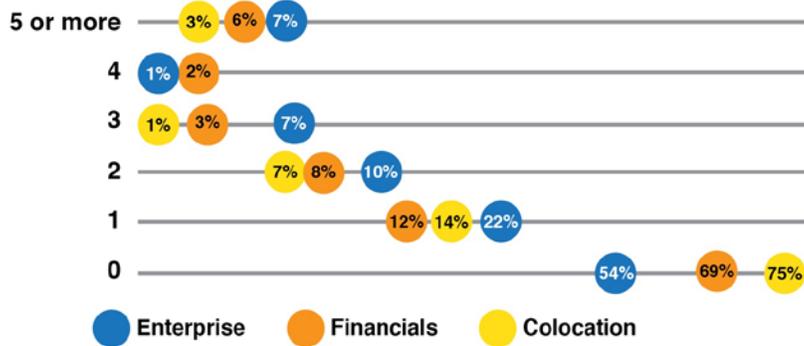


Chart Courtesy of Uptime Institute 2014 Data Center Industry Survey

Does your provider allow remote access to critical electrical or mechanical systems? Can third party service providers employ commands from outside the facility to stop and restart mechanical systems for troubleshooting purposes? With the proper credentials, cyber-terrorists might exploit this feature to shut down these systems either permanently, or long enough to cause overheating, and flooding of the data center.

At the very least, you are going to have some damaged equipment, and depending on the robustness of your DR/BC strategy, you may be out of business.

Study and understand the differences and benefits among different physical security systems and procedures. Are access control and surveillance systems redundant and supported by mission critical network, power, and cooling systems? What accountability measures are in place for security personnel? How are they screened, selected, measured, and rewarded? The answers may surprise you.

5. Contract Risk

Is your agreement form a Lease, License, or MSA? Generally speaking, leases afford you more protection as a client, but may not be available for smaller retail requirements. If you have a lease, is it triple-net, gross, or modified gross? The 'details' of a modified gross lease vary significantly among data center providers.

Is the building owned or leased by your provider? What happens if your provider refuses or is unable to renew with their landlord? Depending on the language in your agreement, you may be forced to relocate with the same provider at your cost. It happened at least twice in 2015, and these enterprises were G500!

Relocation rights, renewal rights, holdover and their time triggers are vital to understanding your options when your agreement comes to term. We have seen agreements with NO holdover or renewal provisions!

At the end of their term, the client was given two options; 1. move or 2. renew under incredibly unfavorable conditions.

Are you intimately familiar with your termination rights, expansion rights, PUE caps, and the conditions of each? We have seen clients in haste, gloss over these details only to find out later that their rights had expired or that they failed to meet the minimum conditions for those claims to apply.

Do you understand what may, or may not be detailed in your agreement related to insurance, consequential damages, simple negligence, gross negligence and limits of liability? Explore with staff and legal counsel the potential scenarios and associated risks. Expect your data center provider to limit their liability exposure as much as possible, however, don't be unreasonable as they will certainly counter with similar obligations for your company. The best agreements are win-win and protect the interests of both parties equitably.

6. Financial Risk

Is your provider private or public? Do they have the balance sheet to support your future growth? Are they capable of funding major emergency repairs and replacements? Do they stock long-lead time critical replacement components as a precaution? Understand their access to capital markets. What are their options? What happens to those options when the market changes?

If the economy flounders will your provider survive?

What if just one segment of the market plunges (i.e. Energy, Retail, etc.) Is your supplier diversified and financially strong enough to weather the storm?

Have you placed ALL of your data center risk (primary and DR) with one provider to take advantage of easier transactions and better pricing? You may consider rethinking that strategy depending on your particular circumstances. Vendor diversity promotes competition and provides experiential contrast by which to gauge performance and progress. If you've chosen a single provider, staggering the terms of your agreements can enhance your ability to negotiate and ease the burden on staff if you do decide to relocate.

Is the data center you plan to occupy leveraged or owned in fee simple? Will they, or can they place debt on the asset you occupy? Does your agreement include a Subordination and Non-Disturbance and Attornment (SDNA) provision? You should know.

6. Financial Risk

Today there are very few reasons for an enterprise to build and own a data center. However, some still do. If you find yourself in this situation, there are ways to maximize the market value of your data center while still providing the protection you need.

Over 90% of self-constructed enterprise data centers have a market value that is a fraction of their book value.

Done properly, a purpose-built data center on a separate parcel of land creates an asset that has real value should you need to extract precious capital from it at a later time. It will be much harder, if not impossible if you've put that investment in your corporate office building, if you've overspent, or created something so bespoke that most would have little use for it.

Engage Experienced Professional Help

Supplement your internal teams with an experienced, unbiased, and dedicated resource to champion a **'thorough'** process, assist in understanding and minimizing risks, and identify the most flexible and economic scenario for your business. Explore multiple scenarios to understand the various costs **AND** risks to your business. Thorough due diligence may be an arduous, time-consuming and political process, but it's a process you don't want impatiently hastened.

"Risk comes from not knowing what you're doing."
"It's better to hang out with people better than you."

Warren Buffett

For more information, please contact:



Shawn Novak
CONSULTING PRACTICE LEADER

DATA CENTER SOLUTIONS | CONSULTING SERVICES

312.297.7631
shawn.novak@cbre.com

CBRE



toward a greener
tomorrow