THE ESSENTIAL GUIDE TO UPGRADING YOUR DATA CENTER

FIBERTOWN

FIBERTOWN

The Essential Guide to Upgrading your Data Center

A quarter of all data center footprint in North America is now outsourced and is expected to increase 15% in 2015. *(DCD-Intelligence)*

The data center is the foundation that houses your critical IT infrastructure, which ensures your data and systems are available 24x7 to both your internal/external users as well as your customers.

There is often a tipping point where your IT infrastructure has become mission critical but your facilities don't meet your requirements. These can be inadequate power, cooling or space. Another driver for building or upgrading your data center is an office relocation. Maybe you're considering a move to a colocation facility.

You've heard about the benefits of colocation – how it can guarantee uptime, provide scalability for infrastructure growth and reduce costs associated with upgrading power and cooling. And you've heard that 25% of the U.S. data center footprint is now outsourced with colocation -- meaning that maybe a facility upgrade isn't necessary.

If you're still thinking a facility upgrade would work better for your business, here is a high-level guide to make sure you consider the key components of designing a world-class data center.

Table of Contents

Power Design

Power delivery is the most critical part of any data center upgrade. Top tier data centers provide multiple power feeds into their facilities, which most likely isn't a financially viable option for a data center located in an office building.

You're first step is ensuring the electrical services to your building are capable of supplying the amount of power necessary for your needs, while giving you room to grow your infrastructure.

Determine your Power Requirements

How much power you require is the single most important part of your data center upgrade. Everything that follows is based off of this calculation…no pressure, right?

If you have a UPS or metered PDUs you can collect the amps/wattage currently in use. If you don't have metered power distribution equipment you will have to do one of the following.

> Option 1: Estimate power consumption based on equipment make and model. Most manufacturers have power calculators that allow you to build your infrastructure online to discover the total wattage.
>
> Option 2: Have an electrician come in and clamp one of the phases of your power. They can then average the usage going to your IT infrastructure.

If estimation is the only means you have available, **remember not to use the rated sticker readings**. The sticker on a power supply gives the potential maximum output and not the nominal wattage the device uses. Often the supply is capable of providing twice the power required to run the equipment. If you go purely off these numbers, you will overbuild your power infrastructure…CFOs tend to frown on this.

Calculating Wattage

If only amperage information is available to you, then you'll need to calculate wattage on your own. Wattage is expressed as Amps x Volts = Watts.

> If your supplied voltage is 120V and you're *using* a total of 40 amps, it would be: 40 x 120 = 4,800 watts (often represented as 4.8 kilowatts or kW).
>
> If your supplied voltage is 208V single-phase and you're *using* a total of 40 amps, it would be: 40 x 208 = 8.3 kW.

Once you calculate required wattage, you can size your UPS equipment, **remember that isn't the entire IT load**. If you're building an application-specific environment, you also need to consider cooling requirements. HVAC equipment isn't run on UPS, but it will be connected to your generator. This will be a key consideration when determining generator requirements.

Learn More

Interested in learning how to audit your power correctly? Chat with one of our engineers live in the bottom corner of **www.fibertown.com** right now.

A Power Versus A+B Power

How much uptime you require will impact your need for A+B redundant power design. The majority of your IT equipment will have dual power supplies. If you have A only power, connecting both power supplies will only provide redundancy for a failed power supply. If a failure or maintenance on your UPS system occurs, you'll experience an outage.

A+B power means you have power fed from two separate sources or circuits. If you have a UPS system for both A and B feeds, then an outage on one power circuit won't affect uptime. Typically, installing A+B power in a data center within an office building is cost prohibitive.

Uninterruptable Power Supply (UPS)

Sizing your UPS is one consideration, but you must also consider what kind of power it will deliver (120V, 208V single-phase or 208V three-phase, etc).

Most IT equipment made in the last 10 years can use either 120V or 208V circuits. Using the calculation Amps x Volts = Watts, you will see that using a higher voltage reduces the required amps to almost half.

At FIBERTOWN, we recommend powering your gear with 208V power. You can load more devices per electrical connection with 208V circuits. Take note, some high-end SANs require 208V three-phase power. If you have a requirement for it, ensure your UPS is up to the task.

UPS Maintenance

Both the batteries and the UPS need to be maintained. Batteries should be tested annually. In a cabinet UPS, each battery in the string should be tested individually. An average battery is designed to last 3 - 5 years before needing replacement; though your mileage may vary. Each time a battery is discharged, its lifespan is shortened.

The unit itself should be maintained also. A certified technician should annually validate the health of the system. This check should include using an infrared camera to validate there are no hotspots indicating an eminent fault. All panels and electrical joints should be verified with an IR camera annually.

Sizing your UPS System

UPS systems are usually rated in kVA (kilo-volt-ampers). This is a theoretical maximum that the device can supply at Maximum voltage x Maximum amperage x Power factor.

Power Factor is the efficiency of your equipment. It's a number between 1 and 0. Large UPS systems were traditionally designed with a PF of 0.8. They are often still designed this way even though newer equipment sports a PF of 0.95 - 0.98. If the UPS is rated at 100kVA with a power factor of 0.8, then the unit can supply 80kW.

On smaller UPS, beware of the rated kVA. These are often inflated or stated in such a way as to confuse you on the actual output.

If you're planning to maintain a backup generator, you only need approximately 2-3 minutes of UPS uptime. A generator can be online and ready to supply power in as little as 20 seconds.

If you don't have the capacity to maintain a generator, you'll need to size the UPS according to how much uptime you need during a power outage. The median outage time across North America is 1.5 hours.

Automatic Transfer Switch (ATS)

An ATS is only necessary when utilizing a generator. It senses when utility power has failed, fires the generator, and transfers the IT load from the UPS to the generator.

Sizing your ATS

To determine the power needs of your ATS, combine the following components.

- The existing IT load
- Anticipated power growth
- The power needs of your cooling equipment.

Determining power requirements should be as simple as matching the breaker sizes you plan to service. If your IT infrastructure is connected to a 200 amp breaker, then you purchase a 200 amp ATS.

Some smaller switches don't always include monitoring capabilities. They might have terminals for dry-contact monitoring, but little else.

These can be retrofitted with CT to measure incoming and outgoing currents and add dry-contact monitors. If you're comfortable with SCADA collections, you can attempt this yourself, otherwise an integrator will need to perform this service. High-end, larger units will generally expose this information via SNMP or Modbus.

Maintaining the ATS

Annual maintenance is required and the ATS should be checked with an infrared camera to inspect all junctions and key transfer points.

All work should be performed by an electrician or certified engineer. This equipment is unfamiliar to most electricians, so having specialized help is a must.

Generator Backup Power

Generators are essential for ensuring backup power in case of a disruptive event. They come in many makes, models and various states of repair. One of the more important decisions is choosing a fuel type: gasoline/diesel or gas/propane.

Fuel Type

In colder environments where generators are outdoors, you'll most commonly use a gas generator with natural gas or propane. Since gas has a much lower freezing point, they are less affected by temperature.

> Small generators often run on gasoline. Gasoline has a lower working temperature than diesel, but isn't as resistant to cold weather as natural gas or propane fuel. Stabilizers can be added to maintain the fuel longer.
>
> Larger liquid fuel generators are most likely diesel. Most of these generators will be skid mounted and can be shipped and dropped directly on a pad. Fuel storage is usually a tank built directly into the bottom of the skid.

All generators are susceptible to cold weather and need to maintain an internal warm temperature to operate well. Diesel systems can have additives to keep them more viscous at lower temperatures. Fuel systems may experience issues including valves freezing, actuator issues, etc.

Monitoring your Generator

Generators don't come out-of-the-box with monitoring services. It's a good rule of thumb to monitor the following conditions.

Running
Is the generator currently running? Every time your generator fires you need to know about it.

Not-in-Auto
NIA means your generator isn't switched to an automatic state. If utility power is lost and your generator is commanded to run, it won't fire unless it is set to *Auto*.

Warning
Warnings can be a myriad of issues, but they allow you to check the generator before they become failures.

Shutdown
Shutdown is any error that will prevent the generator from firing (low oil, low coolant, over crank). This error you will have to manually address.

Fuel
Some generators may be able to alert on low fuel levels, but trending actual fuel levels is invaluable for predicting refueling or indicators of fuel issues.

Maintaining your Generator

WEEKLY: Generators should be exercised regularly. Generally, a weekly run schedule is employed. Often a generator will run for 30 minutes during a testing phase.

MONTHLY: It's recommended that a monthly load test is performed. In these situations, a generator is fired and the ATS is manually switched to generator. This forces the generator to carry the IT load. Once complete, the process is reversed and all settings are put back in auto. A load test stresses a generator more heavily. The added load will increase the temperatures in the exhaust system and burn off any lingering hydrocarbons.

QUARTERLY: A certified technician should inspect your unit quarterly and change the engine oil. During these events, the generator will be put in shutdown mode, which means **without an N+1 power configuration you run the risk of outage**.

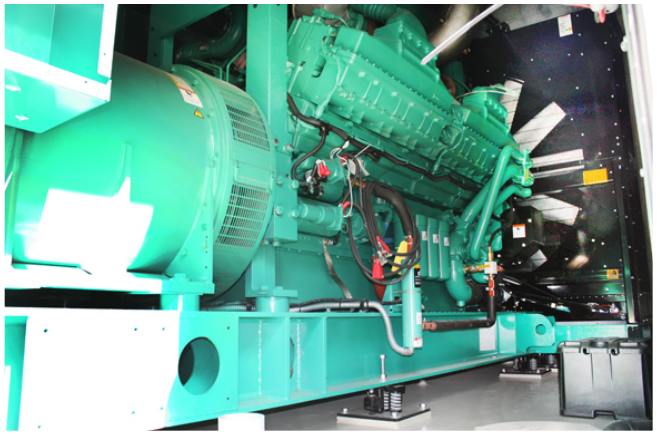
ANNUALLY: Generator batteries should also be closely monitored and replaced every 3-5 years. Deep cycle sealed batteries are recommended. More cranking amps will be to your benefit in those cold months.

As per your manufacturer, schedule any plugs, filters or coolants that need to be replaced.

Cautions

Step one when working around a generator is to put it in manual or emergency stop. The last thing you want is for it to fire while you have your hand anywhere near the unit.

Whenever working around generators be sure to wear hearing protection. After any maintenance is performed you should run through a "back in auto" checklist to ensure all systems are prepared to carry the IT load.



Did you know?

The industry average is nearly three outages per year from natural disasters, human error, power outages or routine maintenance. Check out our infographic on the **Impact of Data Center Downtime.**

www.fibertown.com/offers/info-data-center-downtime

Cooling Infrastructure

Dedicated cooling is necessary for redundancy. Even if your office HVAC system can support the IT load, you'd have to size the ATS and generator large enough to accommodate the additional load from the base building cooling. A dedicated cooling system for an office data center won't be as demanding as the building HVAC and easier and less expensive to connect to your ATS and generator.

Is raised flooring necessary in your data center?

This is often determined by size and budget.

Raised flooring is generally 2' x 2' concrete and steel tiles raised 24 – 36 inches off the floor. Cool air is forced under the floor and escapes through specially designed perforated tiles. This allows you to target precisely where you want cool air to escape. Hot air is collected near the ceiling and returned to cooling units to be fed back under the floor.

Raised flooring is pressurized underneath by the volume of cooled air forced under it. If a single unit is taken offline, remaining systems will continue to cool and feed all remaining areas of the room.

Raised flooring also allows for power and connectivity services to be ran under the floor and out of the way of equipment.

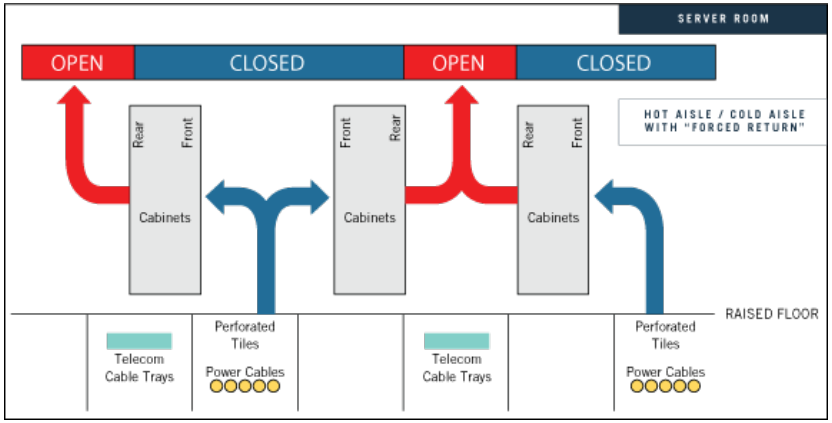
Bare concrete is the less expensive option, of course. In a small data center, it may not make sense to go to the trouble or expense of installing raised flooring. With concrete, you'll have to feed cooling overhead and attempt to duct it into your cold aisles.

Return can be performed by pulling ambient air, chimneys or containment. Some local fire codes may have special requirements for these environments.

Ambient return is more effective in a raised floor design as the cool air isn't feeding near the return. With bare concrete, ambient tends to work best in small areas.

Chimneys are specialized cowls attached to the discharge side of a rack. They're designed to funnel hot air up or directly into a plenum.

Containment can be done either via hot aisle or cold aisle. Cold aisles will use special damning material (fire resistant plastic) to contain all of the cold air on the cold side of racks. The rest will be open and considered hot return. These rooms are generally quite warm. In hot aisle containment, the room is kept cold and all of the hot areas are duct into a return.



Cooling System Types

Water Systems

Water-based cooling systems require an outdoor chiller and pump with indoor variable frequency devices, controls, CRAH units, and filter and leak detection.

Chillers

- Chillers are a pack with fins and fans. Fan blades are regularly lost and frequent repairs are needed.
- It's necessary to ensure chillers don't shut down in cold weather. With a lead and lag chiller, water must run constantly and special mechanisms must be in place. Cold climates require a glycol mix, which makes the system higher maintenance and more expensive.
- A failure within a single unit will result in cooling loss. A backup chiller is required for 2N redundancy.

Pump

With a chilled water loop, an outdoor pump is required to keep the water flowing. If this unit fails, you'll lose cooling. A backup pump should be considered.

Variable Frequency Devices (VFD)

VFD are what control the speed of the pump. If you have multiple pumps, you'll need multiple VFD.

Controls

Controls maintain the temperature of the chilled water loop. It will command the chiller on, control the orientation of valves, control the speed of VFD, monitor differential pressures, maintain status of temperature probes throughout the loop and monitor flow rate.

Filters

Chilled water loops require filtration. A *sock* is typically installed and must be maintained.

Leak Detection

Flowing water requires leak detection around joints and cooling units.

Gas Systems

Gas systems are similar to the cooling systems at your home. These are typically smaller units. Each indoor unit will correspond to an individual outdoor condenser unit.

Because this is a gas system, freeze protection is less of a concern. These systems can be used for large deployments and will be less expensive than a chilled water system.

The indoor cooling unit controls the operation of the outdoor condenser unit, which means less system intelligence is required.

For small office data centers, this option will supplement your cooling as it is simpler to retrofit and is less expensive.

Computer Room Air Handlers (CRAH)

CRAH units take warm return air near the ceiling and blow cold air out the bottom of the unit near the cabinets.

These units come in multiple styles and cooling ratings. Raised flooring units will feed cold air directly from the bottom of the unit. Hot air will be brought in through the top of the unit. Bare concrete units will often duct from the lower portion of the system.

In large environments, CRAH units are connected so they act in unison, this prevents one unit from humidifying and the adjacent unit attempting to compensate. Multiple units are necessary when designing N+1 or better redundancy.

More sophisticated units will come with A+B power capabilities. Again, cooling must be running during equipment maintenance and not only during outages. This allows one power feed to be manipulated while maintaining temperature.

Cooling System Maintenance

If you run a chilled water loop, it must be sampled and tested biannually to ensure proper water balances.

If you run a glycol system, it must have its levels checked regularly as glycol puts a heavy burden on the plumbing.

- Filters in chilled loops must be checked biannually. Chillers must be maintained biannually to ensure all blades are intact, motors are rotating properly, sensors are function, and valves are operational.
- Condenser units must ensure they are clean and operating properly and efficiently.
- CRAHs should be serviced quarterly to have units inspected and filters changed.
- Thermal imaging should be done annually to ensure cooling delivery and return is operating at peak efficiency.

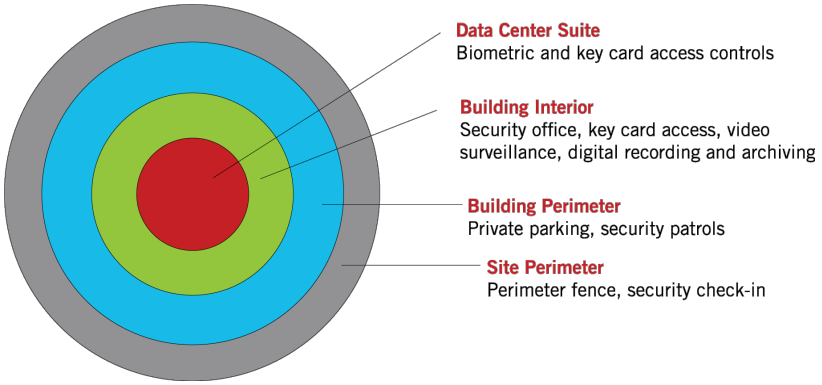
Physical Security

Security is often overlooked in office data center environments. It's important to consider to what level you need to secure your facilities, who will have access, who will have keys, what are the available access hours, do you require regulatory compliance?

Colocation data centers employ multiple layers of security including gated entry, parking lot patrols, security office check-in, mantraps with key card access, biometrics and video monitoring. They also maintain annual audits with SSAE 16 SOC 2 certification.

In small office environments key only access may work and keeping an entry/exit log may satisfy compliance requirements. If an employee is let go or resigns, what will be your policy? Do you take ownership of the key, do you rekey the door, are you using specialized keys that aren't easily duplicated or are costly to duplicate?

You may want to consider keyless entry to alleviate some of these issues. While maintaining the highest level of accountability, you will need a dedicated access control system for a keyless system. The best thing to do is create a prioritized list of what you require from the system.



Access Control Checklist

Scalable system

- ❑ Will this grow with me or am I locked in at a set size?

Open system

- ❑ Am I able to administer users?
- ❑ Am I able to make adjustments to schedules?
- ❑ Am I able to adjust clearance profiles?
- ❑ Am I able to add new hardware to the system?
- ❑ Do I have access to the database?
- ❑ Can I create custom reports?
- ❑ How much can you do without being locked out?

Reporting

- ❑ Can I run reports on individual users?
- ❑ Can I run reports on individual doors?
- ❑ Can I run reports on groups?
- ❑ Can I run reports on user configurable criteria?
- ❑ How long is information stored?

Alerting

- ❑ What alerts are configurable?
- ❑ Door propped
- ❑ Repeated authentication failure

Operations

- ❑ Is this affordable?
- ❑ Is biometric authorization and fingerprint scan needed?

Connectivity

Whether it's delivering high volumes of data or connecting multiple offices, Internet and WAN connectivity are essential to your IT infrastructure. The first step is determining what services are necessary for your business.

- Direct Internet Access
- MPLS
- Metro services
- Transport to other locations

Step two is determining what carriers are available. You may have multiple carriers connected to your office that satisfy your requirements. However, it's always a good rule of thumb to evaluate multiple telecom providers, especially ones that own the fiber.

The key to redundancy is fiber services from multiple providers, or at a minimum multiple paths into your facilities from a single provider.

Look at carrier maps for major Tier I carriers and ask around via your municipalities who has fiber in the area. Another good resource is any school districts or universities as they generally quote connectivity from multiple providers.

Lastly, evaluate how much build-out you would have to do to meet carriers at their nearest splice point, or how much it would cost to have them put connections directly into your building.

Did you know?

Most colocation data centers are built along major fiber inter-exchanges to deliver the lowest latency and most robust connectivity to data center customers. Carrier-neutral facilities provide high-performance networking options for maximum reliability and redundancy. You choose the best carrier and solution that works for your business.

Network Design

There are multiple ways to build a highly available network. Let's assume you require a 100% concurrently maintainable network, which ensures when any one connection is lost you can maintain network connectivity.

Internet Service Provider

If you maintain multiple connections that end users must access 24x7, you can achieve connectivity through DNS and BGP.

Adjust Domain Name Servers (DNS)

Consider what happens if you have two separate carriers providing diverse IP subnets and your end users are accessing them via DNS and your primary carrier fails? Your users will attempt to access unavailable services.

To avoid those situations, set the time-to-live on DNS entries to five minutes ahead of time, which will allow you to change the IP addressing. As the updated DNS propagates, it will allow your users to slowly adjust.

There are automated DNS services such as UltraDNS, which monitor external services, detect a failure and automatically adjust DNS entries. The advantage of an automated system is that it performs failover at any time and you can expect a failover of roughly 5 minutes.

Border Gateway Protocol (BGP)

BGP is a dynamic routing protocol that controls the flow of information on the Internet. BGP allows you to influence the flow of traffic both in and out of your network and is preferable to DNS management.

An Autonomous System Number (ASN) is assigned via a local registry. This ASN allows you to peer with upstream providers. You can advertise your registry-assigned IP addresses with your primary and secondary ISPs. If one ISP fails, the identical addresses are available via your secondary ISP.

Hardware

Multiple connections should be hosted on multiple routers to maintain connectivity should a single router fail. Border routers can then be connected to redundant firewalls. From the firewall, you should have connectivity into a pair of core switches for layer 2 aggregation.

Can you see the pattern? For max redundancy, host connectivity on multiple devices from beginning to end. Often this configuration can be collapsed where multiple functions are performed via a single piece of equipment. Your required uptime should be balanced with cost.

Monitoring

The final piece of a highly available data center is asking how you know that it's operating as it should? Did utility power kick on at 3 a.m. and the generator fired? Does the UPS have a critical condition? Here are the key elements to monitor.

Power Monitoring

Most UPS systems have state information available via SNMP, including traps and syslog messages for alerting. Trending and altering on the following information is key.

- UPS battery state and charging state
- UPS battery charge level
- UPS run time available
- UPS power input
- UPS power output
- ATS input sources in use
- ATS supply voltage/amperage from the active source

Whips

Power usage can be monitored at the whip level via branch circuit monitors (BCM) or power distribution units (PDU).

BCMs are hard circuit transducers attached in the breaker panel for each whip. These are often monitored via Modbus RTU, though a Modbus TCP gateway can be used.

PDUs are intelligent inter-cabinet power strips that are easy solutions for small environments. You can measure current via SNMP on these units. This will allow you to trend utilization over time and ensure proper operation of A+B whip pairs.

Cooling Monitoring

The majority of CRAH units come equipped with SNMP capable monitoring cards. Trending this information can be extremely useful for efficiency tuning.

- Set points for temperature and humidity
- Current state
- Cooling on or off
- Current temperature
- Humidifying/dehumidifying
- Current humidity level (AHSRAE 20-80%)

Temperature

It is important to measure temperature at the CRAH units, but also via ambient probes. This will give you a good idea of conditions for data center equipment. A minimum of two probes should be used for comparative reasons.

Considering Colocation?

Make sure to ask what monitoring services the data center provides. Most high performance facilities track power and cooling performance and offer device monitoring for an additional fee.

Download our **Colocation Checklist** to compare providers and ask the right questions.
http://fibertown.com/offers/colocation-checklist

Network Monitoring

A network environment without monitoring is completely reactive. By monitoring multiple connections and collecting messages from devices, you can reduce your break-fix time in half.

Network Equipment

Each piece of equipment that contains a network interface should have its bandwidth monitored. For example, if you suddenly experience server issues and monitoring shows the port has its interface bandwidth maxed out, you can quickly eliminate many potential issues.

Hardware

Memory, CPU and hard drive utilization should be monitored and altering thresholds established. If a border router's CPU is maxed out for at least 5 minutes, this is an immediate concern.

System Alerts

Syslog collection and alerting is another best practice. Setting this up will alert on events from multiple devices:

Network

- ❑ OSPF routed event
- ❑ BGP routed event
- ❑ HSRP event
- ❑ Lost power supply
- ❑ Down serial interfaces

Server

- ❑ Lost hard drive
- ❑ Lost power supply
- ❑ Administrative user login
- ❑ Failed login attempts
- ❑ System/service errors

Firewall

- ❑ Shun events
- ❑ Login failures
- ❑ VPN user login

Houston's Most Trusted and Respected Data Center

Businesses require a data center that provides accountability and delivers excellence 100% of the time. FIBERTOWN is an extension of your IT team and involved every step of the way. You will know each of us from executive to technician because we are passionate about providing high performance colocation services creatively designed to fit your needs. Locations in Houston and Bryan, Texas.

FIBERTOWN

www.fibertown.com