


SECURE360
conference
DATA PROTECTION STARTS
WITH PHYSICAL SECURITY

Kenneth G. Hartman
Security Architect
OneNeck IT Solutions

 Like what you hear? Tweet it using:
#Sec360

KENNETH G. HARTMAN

Security Architect, OneNeck IT Solutions
CISSP, CPHIMS, GISP, GSEC, GCIH, GCIA

Kenneth.Hartman@OneNeck.com

www.OneNeck.com

www.KennethGHartman.com

[@KennethGHartman](https://twitter.com/KennethGHartman)



Elevator Speech:

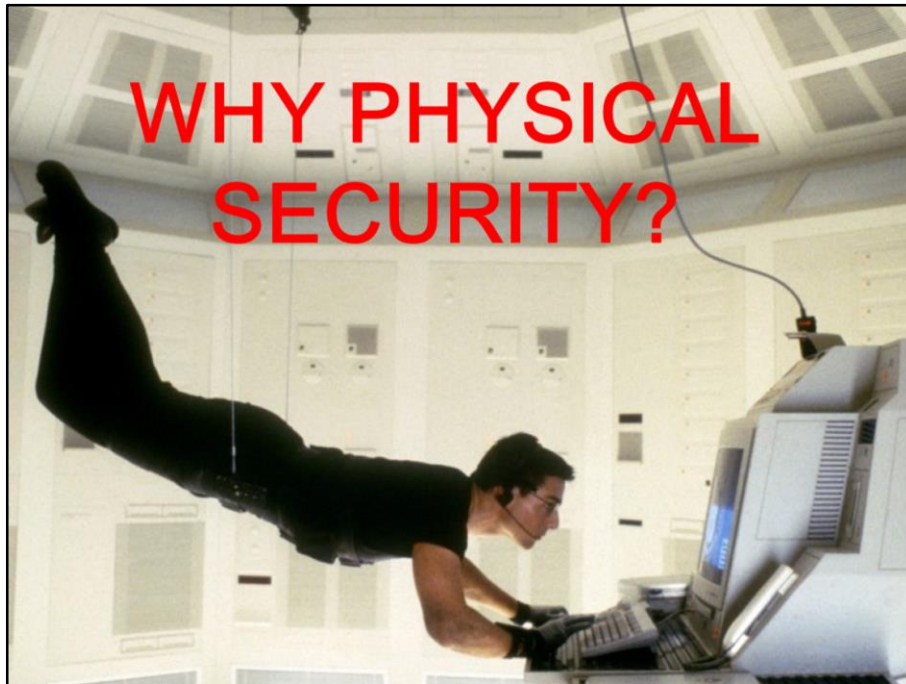
"I help my organization earn the trust of its customers"

Like what you hear? Tweet it using:
#Sec360

I'm Ken Hartman, a Security Architect for OneNeck IT Solutions. OneNeck is the growth services arm of TDS, providing Colocation, Cloud, Managed Services. We are also a Value Added Reseller.

**

Elevator Speech: *"I help my organization earn the trust of its customers"*



Let's face it, physical security is not as cool and hip as Hacking or Trojans, and Viruses, and other Malware. Physical security topics typically do not rock the media like was the case with the Heartbleed OpenSSL vulnerability or the latest zero day exploit.

However, if unauthorized people have physical access to your server, you may not have any security at all. Today, we cover the nature of physical security threats and the Security controls that a modern, state-of-the art commercial data center uses to mitigate these threats and offer a 100% SLA.

Physical attacks can include things such:

- Simply hitting the reset switch or power button
- Using a flash drive to steal data
- Destroying or stealing important system components, (Hard Drives)
- Theft of an entire server

DISCLAIMER

I am not a salesman and this talk is not a sales presentation. Most organizations are not permitted to not talk about their security features, because they do not want those features exploited or the information that was shared used against them.

This talk will use specific examples from my company, Oneneck IT Solutions, simply because *I am authorized* to talk about the ones that we will discuss today.

You will not hear very many references to OneNeck, but I do want you to know that I am talking about real data centers, one of which is located in Madison, Wisconsin





I tend to take a fairly academic approach to defining concepts, and use them with precision. I find that this creates improved understanding and avoids misplaced trust.

IT'S ABOUT DAD...



Disclosure
Alteration
Destruction

...and Safety

Security is all about Risk Management

As you all know, information security is about managing threats involving:

- Disclosure of Sensitive information (breach of confidentiality)
- Alteration of that information, so that one cannot rely on its integrity
- Destruction of that information or disrupting its availability

DAD => Confidentiality, Integrity, Availability

What is it about your information that makes it valuable?

--it is that the right people can access that information when needed and that the wrong people cannot

Authorization is the process to define *who* the “right people” are....and

Access Control is preventing the “wrong people” from accessing that information

Physical security may also involve managing risks to personnel safety and in some organizations the physical security team is also tasked with loss prevention (theft of products)

Since this talk is focused on data protection, we will be focused on risks to confidentiality,

integrity, and availability

SECURITY CONTROLS

Control - a *control* is any administrative, managerial, technical, or legal method that is used to modify or manage information security risk.

Controls can include things like:

- practices
- processes
- policies
- procedures
- programs
- techniques
- technologies

Controls are sometimes also referred to as *safeguards* or *countermeasures*.

<http://www.praxiom.com/iso-27000-definitions.htm#Control>

Everyone tosses around the word “security control” but not everybody has a clear definition of what is meant by that word.

One more definition, a few concepts and then we will jump into the good stuff.

CONTROL OBJECTIVE

Control Objective- a *control objective* is a statement about what your control is expected to achieve

- Each control is selected to achieve a specific result
- A Security Control is intended to manage a specific risk



Security controls are selected as part of an intentional *risk treatment process* to address specific risks that are identified during a risk assessment.

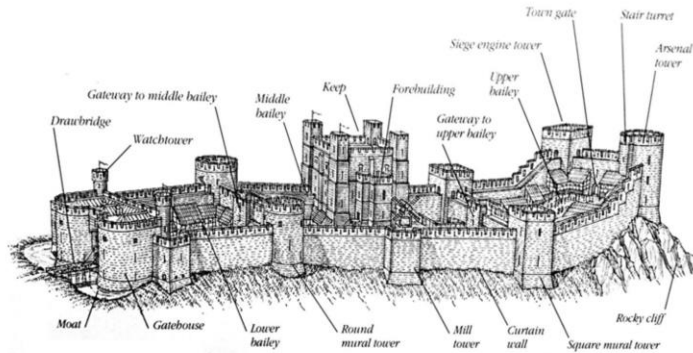
I keep using the word specific, because I want to emphasize that a given control is intended to achieve a specific result (control objective) and not understanding the control objective, can result in misplaced trust, security incidents, or ineffective incident response.

Example:

Think for a moment, about the control objective of a security camera. Does a security camera **prevent** a bad guy from entering your restricted area? No, but it may **deter** them. Is a security camera a **detective control**? Maybe, but only if you have someone watching the camera 100% of the time. Most organizations use security cameras as a **Forensic Control** – to determine, after the fact, what actually happened.

If you define your control objectives, this adds focus to your control testing (your auditing). You can then verify that the security control meets the control objective!

DEFENSE IN DEPTH



A castle is often used during security awareness training to describe the concept of defense in depth. But what really is Defense in Depth? Is it really just overlapping controls? Or is it really aligning control objectives as well—making sure that no gaps and considering what happens when a control fails.

In security, we have a saying “Prevention is good, but detection is a must!” Design your detective controls to augment and overlap your preventive controls. For example, use a motion detector behind a locked door.

The title of this talk is “Data Protection Starts with Physical Security.” You do not have data security if you do not have defense in depth—starting with the physical security of the data centers that house your sensitive data.

Shortly we will start discussing the physical defense in depth features that are applied in one of our data centers, but first one more concept that was driven home during our ISO 27001 certification journey...

PLAN – DO – CHECK - ACT



PLAN—Prepare a written action plan that covers what you will do and how you will do it.

DO—Work the plan. Start with a pilot project or test case. Communicate issues and learning. Revise the written plan if needed.

CHECK—Test your solution per the written action plan, but test creatively as well. Determine what “breaks” your solution.

ACT—Request corrective actions on significant differences between actual and planned results. Analyze the differences to determine their root causes.

<http://www.kennethghartman.com/plan-do-check-act/>

Excellence does not happen by accident. It is the result of sustained focus and attention to detail.

Much of what I am about to show you is the result of continuously improving the security controls over several years by many very talented folks.

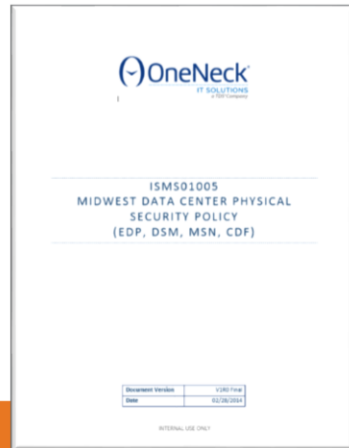
Each data center phase incorporates the industry best practices and all of the learning from our Plan-Do-Check-Act cycles.

Like many data centers, OneNeck uses third party auditors during the “check” phase



Policies and Procedures are administrative controls.

POLICY & PROCEDURE



Sample Requirements:

- Proximity Card & Biometric Scan
- Magnetic Locks
- Mantraps & tailgating detection
- Door Held Open Alarms
- 24 x 7 x 365 Video Surveillance
- Access Logs
- Door Alarm Audits

How do policies make you more secure? They document management's expectation about how security is to be implemented and create the "Mandate"

Procedures describe how those expectations are actually to be implemented and create the standard to be audited against.

Although InfoSec is often tasked with the responsibility to write the policies and procedures, do not take this responsibility lightly...after all you have the power of the pen...So use it to design your future state and articulate what the business needs to accomplish to appropriately manage its risks.

For Information Security to be effective, you need to generate a strong mandate. Policies can help you facilitate that.

Create a Mandate...

WE ARE ON A MISSION...!



On my team, we have been evoking Blues Brothers Imagery, and we proclaim that “we are on a mission!”

Information Security can be tough, and thankless. And Physical Security isn’t necessarily glamorous.

We have a mandate and the important task of securing an important business unit of a Fortune 500 company

We don’t have time to screw around with bureaucratic resistance to change

It is amazing how the right imagery infuses energy into a team and even reminds them that it is ok to enjoy your job



BUSINESS CONTINUITY PLANNING

1. Policy & Framework
2. Risk Assessment
3. Business Impact Analysis
4. Biz Continuity Strategy
5. Biz Continuity Plans
6. Test & Update



Who here enjoys business continuity planning? Its kind of like planning your own funeral.

As we set about formalizing our business continuity planning process, I did receive pushback

- We do not want a paper dragon!
- We don't need a BCP, we sell DR Services! It's what we do
- We need to make sure that our customers do not think that our BCP is their BCP because our contracts state that each customer is responsible for performing their own Biz Continuity planning

In Plan-Do-Check-Act fashion, we started by creating a policy and a framework. During the Risk Assessment process, we determined the qualitative probability and impact of various environmental events like snow storms, earthquakes, tornados, as well as technical threats and supply-chain related risks using a list from a BCP planning website I found on the Internet.

BUSINESS IMPACT ANALYSIS

KEY ACTIVITIES THAT SUPPORT COLOCATION

- Control Physical Access to Colocation Customer Equipment
- Provide Power to each Colocation Customer
- Provide Internet/Private Network Connectivity to each Colocation Customer
- Provide Controlled Temperature & Humidity to the Colocation Data Rooms
- Provide Fire Protection to the Data Room



"Hedgehog Concept"

After the risk assessment, we performed a Business Impact Analysis. Since this isn't a talk all about Business Continuity Planning, I will spare you of the detailed steps that we performed.

One of the results of the Business Impact Analysis was the determination of the Key Activities that support each critical business function. Here are the Key activities that the Data Center must provide for its customers.

The Business Continuity Planning Process is still about managing risks to Confidentiality, Integrity, and Availability, with a focus on Availability of course.

In his book ***Good to Great***, Jim Collins introduced the "Hedgehog Concept" -- Doing One Thing and Doing it Well.

Defining your Key Activities gives clarity of purpose. Clarity of purpose becomes powerful when fueled by your mandate!

I have grouped our physical security controls that we will be discussing next into these 5 key activity areas.

BUSINESS CONTINUITY STRATEGY

Business continuity at OneNeck is an encompassing process built on the philosophy of **design for high availability** solutions in a **stable environment**, with **defined processes to manage situations** that threaten the ability to sustain service.

Our Services are designed to deliver services at a specified availability Service Level Agreement (SLA) which we contractually commit to.

Furthermore, our contracts typically contain language that states that the client is responsible for all backup, nonstandard data protection, hot site, disaster recovery and other similar services designed to protect Client's systems, software or data. Note that the obvious exclusion to this would be if the customer obtained backup or disaster recovery services from Oneneck is an executed service order.

OneNeck does not attempt to mitigate against Force Majeure Events beyond what is typical and customary among our industry peers.

Once we defined and articulated our Business Continuity Strategy things fell into place.

All of things that we were doing right in the design and operation of our highly resilient data centers could now be applied in our BCP.

I share this because our approach to business continuity planning is not the same as it is in a traditional IT world, but it is common in our industry

UPTIME INSTITUTE – TIER 3

Concurrently Maintainable Site Infrastructure

- Redundant capacity components
- Multiple independent distribution paths
- All IT Equipment is dual-powered
- 12 Hours of on-site generator fuel
- Each component can be removed from service without impacting the critical environment
- Sufficient permanent installed capacity when redundant components are removed

<http://www.uptimeinstitute.com/>



UPTIME INSTITUTE – TIER 4

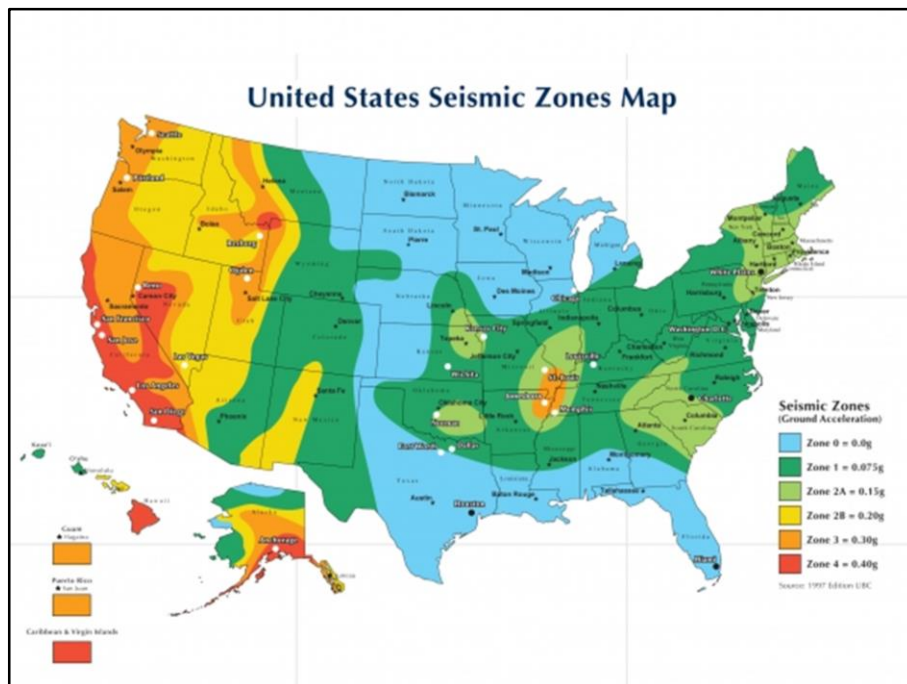
Fault Tolerant Site Infrastructure

- Multiple, independent, physically isolated systems
- Multiple, independent, diverse active distribution paths simultaneously serving the critical environment



What I like about the Uptime Institute Tier Standards is it allows the data center owner to decide what level of resiliency that they want to design to.



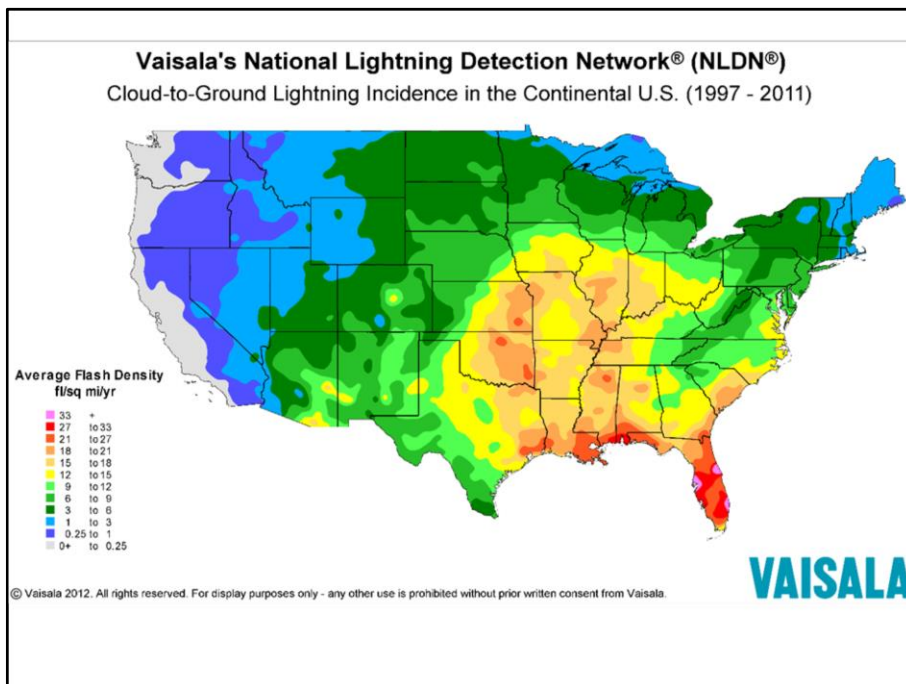


Although unauthorized access is a concern, you also need to protect your business against environmental threats. A fire, flood, or tornado could be just as damaging to your business as a data breach (if not more so).

Understanding the environmental threats most likely to your business is critical if you're to understand which controls you should invest in.

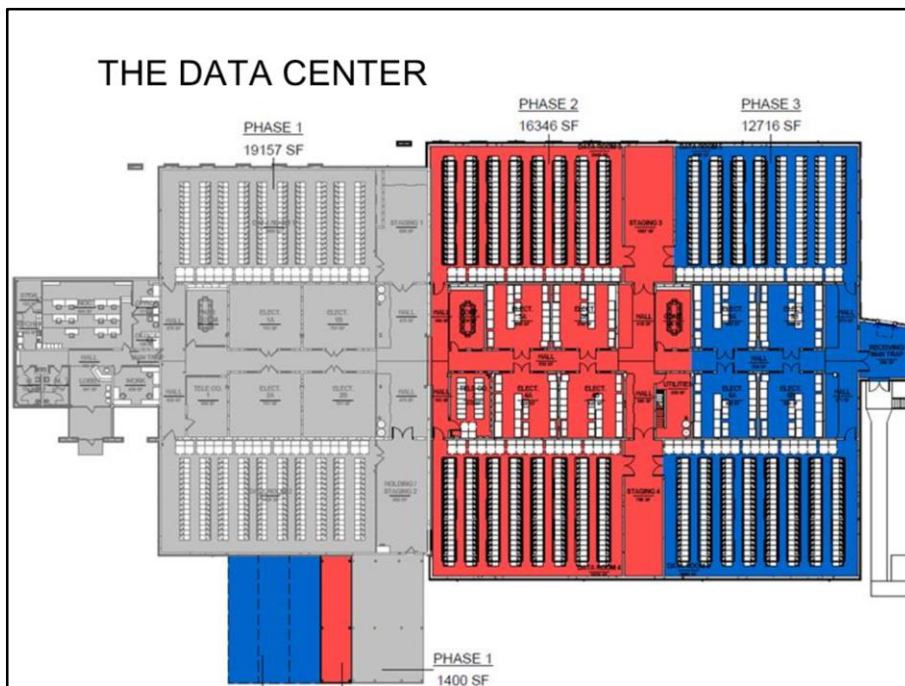
We are Siesmic Zone 0 out of 4

The building is constructed so that it can withstand a direct hit from an EF4 (166-200 mph) tornado



We are also in a low lightning incidence area and have proper lightning arresters in place on the building

Flood plains and similar factors are all considered in locating your Data Center



\$35 million, 55,000 square foot, state of the art data center, the largest commercial data center in all of Wisconsin

Phased design

All mechanicals (and electrical) can be serviced in one main corridor – AWAY from customer racks. No overhead pipes, no technicians accidently dropping a screwdriver into a rack.

Reception - Kitchen -- Telco Rooms -- Staging Areas

SECURITY ZONES

- **Common Area** – non-restricted areas of general business use not requiring a proximity card (e.g. lobby reception area)
- **Office Area** – Level 1 Restricted Areas with direct non-public network access requiring proximity cards or escort by valid proximity card holder (e.g. employee workstations, interior conference rooms located within restricted areas).
- **Data Room** – Level 2 Restricted Area within the Data Center which houses company or customer telecommunications or computing infrastructure used in storing, processing, or transmitting data.
- **Critical Area** – Level 3 Restricted Areas with additional limitations on unescorted access due to the presence of systems or infrastructure that are paramount to the operations of the Data Center (Teleco, Utilities)

Common Area == Reception Lobby, prior to check in

Office Areas == Customer amenities include conference rooms, work rooms and kitchen access, as well as a staging area.

Each customer is granted access to only the data room their systems are in (Six Total)

Critical Areas require a Data Center Technician to escort. (i.e. Telco Room & Electrical Rooms)

RECEPTION AREA



Inner doors of the vestibule are locked, so a guard has to let you into the building.

Once inside the reception area, the guard will check you in with a government issued photo id or a proximity badge

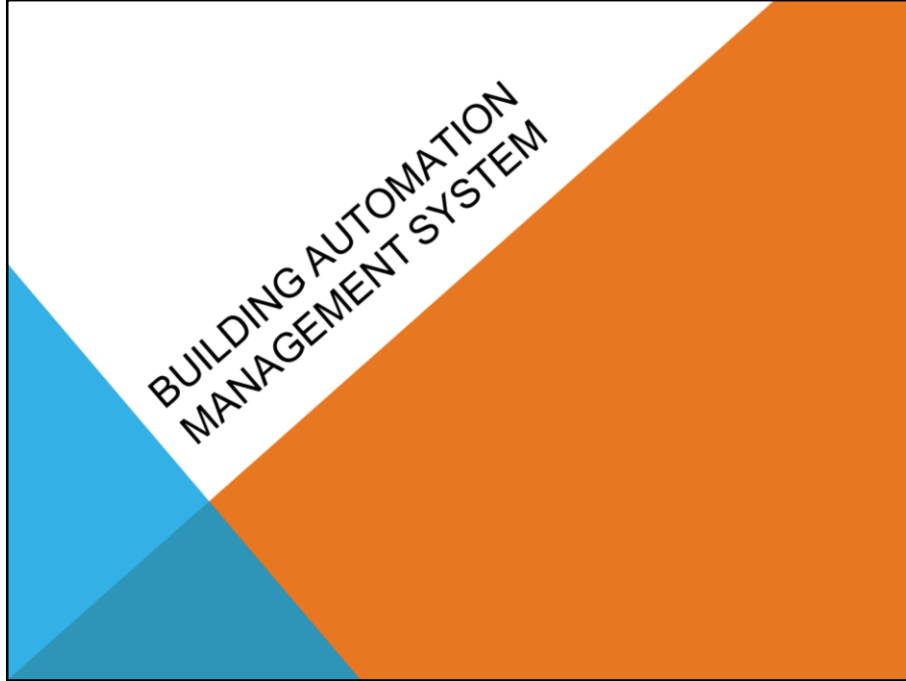
The building is staffed 24 x 7 by security guards

Over the shoulder of the security guard, is the Facility command center

FACILITY COMMAND CENTER

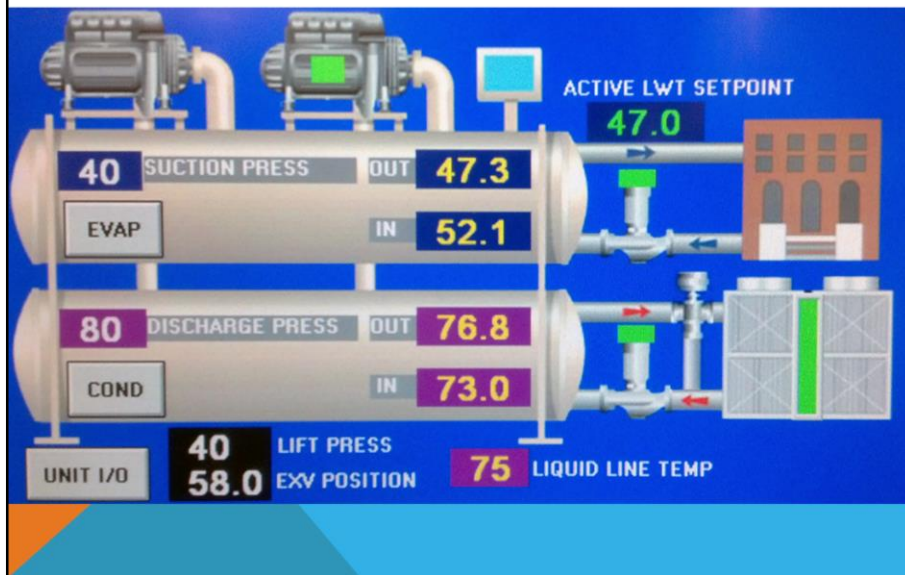


The facility command center is where many of the alerts, messages, and monitoring systems for the facility are displayed.



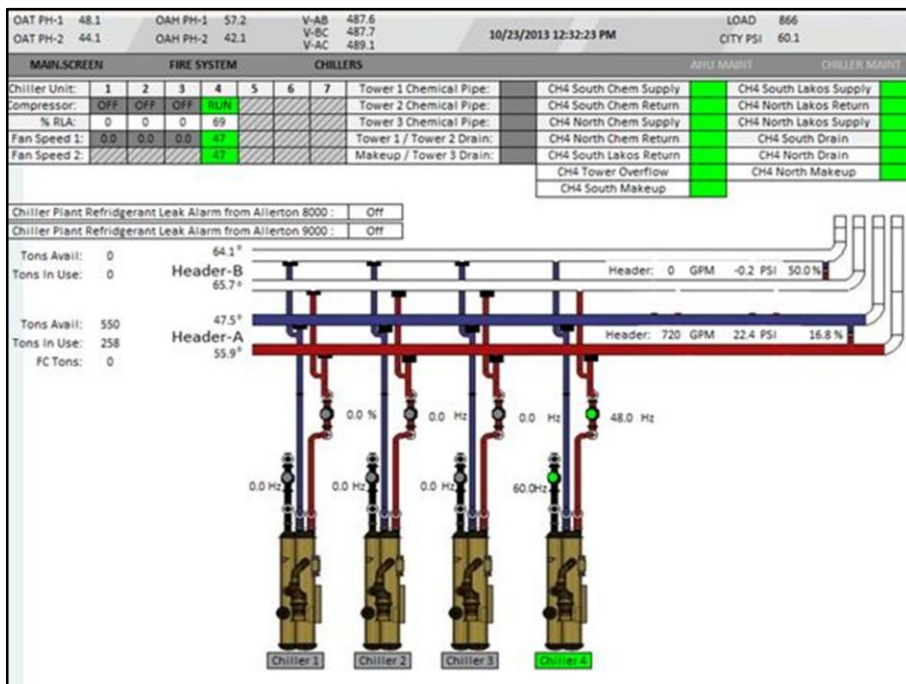
The messages, alerts, and monitoring is performed by our Building Automation Management System ("BAMS")

BUILDING AUTOMATION SYSTEM

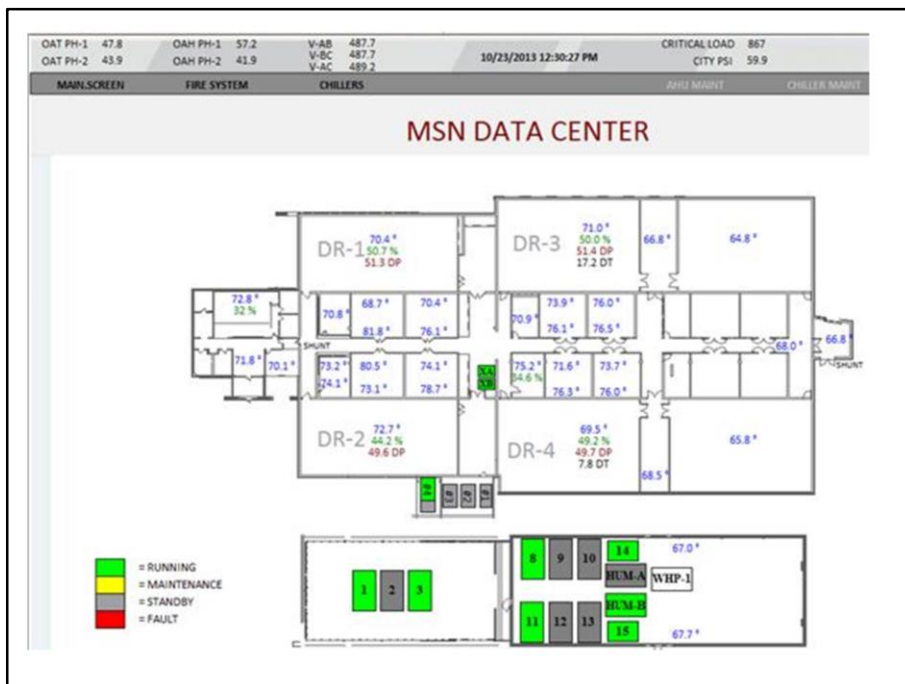


One of the best ways to detect when an event occurs is to monitor the health of your systems. We use a BAMS to monitor and control all data center assets

Andover Controls -- we have over 2500 sensors throughout the building (10,000 I/O points) which ties back to our Facility Command Center and automation network. The BAMS ties alarm notifications into a trouble ticket system to schedule proactive maintenance and can issue pages to appropriate personnel when an adverse situation occurs.



The BAMS controls all the HVAC functionality.

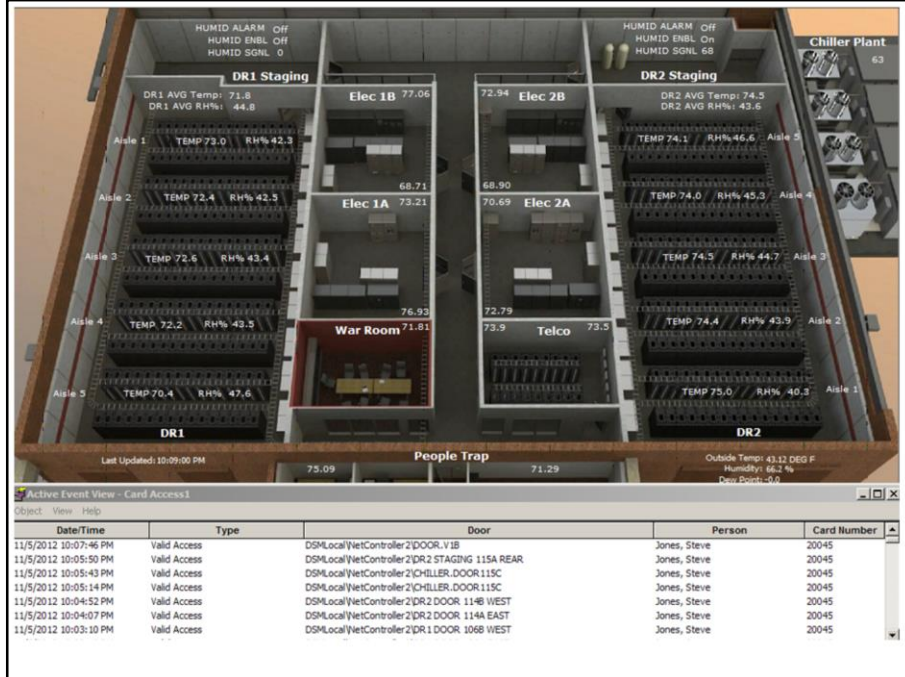


There is also various views of the facility. This one shows temperature and humidity.

I included this one because it shows a nice floor plan of the facility, including the second level, which just covers the central corridor.

Each area is clickable to drill down for more information





This 3-D view from the BAMS is a nice view of the Phase 1 portion of the facility.

People Trap

Data Rooms 1 & 2

The Electrical Rooms for each data room (2 each) More later

A conference room for meetings and disaster recovery exercises

Telco Room

This picture also shows some badge access logs at the bottom.

MULTIFACTOR AUTHENTICATION



We require an Iris Scan in addition to a proximity badge to move between restricted areas. So basically, one has to have a scan before entering any of the data rooms or the telco rooms from the central corridor, or to enter the main corridor from the reception area. This is a counter measure against badge-sharing. {Remember each control is to mitigate against a specific risk.}

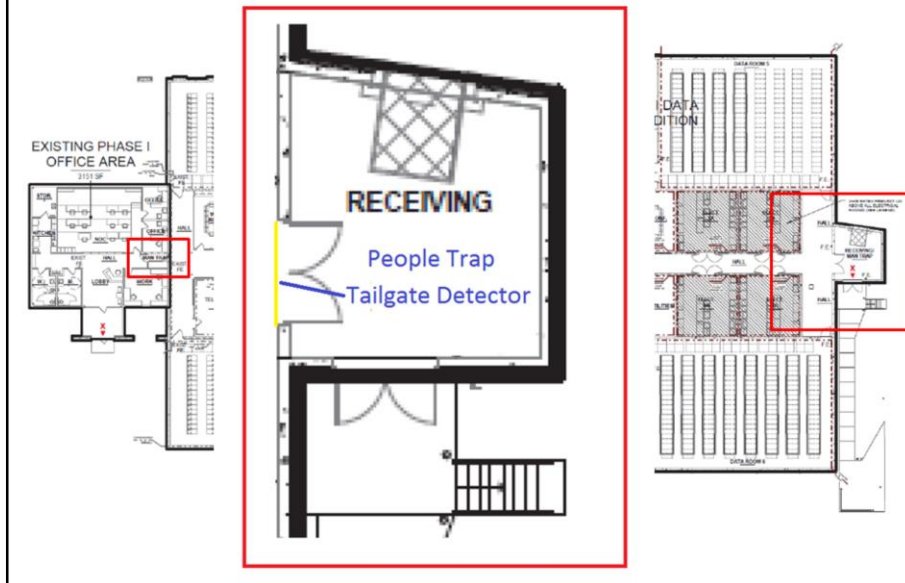
Again, people are authorized to access only the restricted areas that they need to perform their job or access the systems they own.

PEOPLE TRAP & TAILGATE DETECTION



We have two man traps ("People Traps") if you will.

PEOPLE TRAP & TAILGATE DETECTION



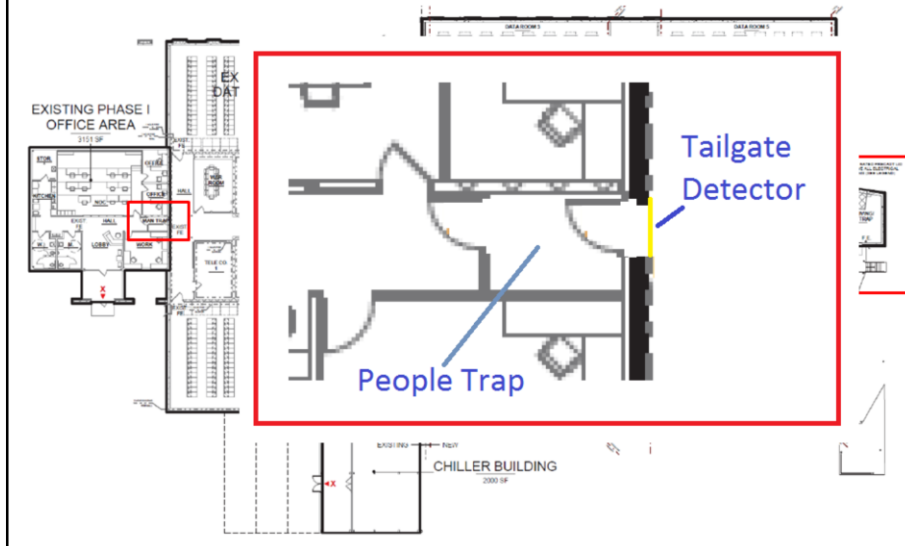
The people trap consists of two doors. The way that it works is a person will scan their proximity badge, open the door and enter the vestibule. Once the door is closed, the person will badge one more time and scan their iris which will then unlock the second door.

Under normal conditions, only one person is allowed into the man trap at a time. To enforce this, there is a “tailgate detector” that emits an audible alarm if it detects that more than one person exits the people trap after a scan.

Exception: Tours – 1 badge holder employee for every 5 visitors. The tailgate detector still goes off, but the guard is aware of the tour and it is an expected condition.

An alarm log entry is made for each badge scan, the iris scan, and any tailgater alarms.

PEOPLE TRAP & TAILGATE DETECTION



We use a second people trap in our receiving dock area. This room actually has two different types of receiving doors, one is a regular double door but the other is a roll-up door with a dock leveler. A third set of doors are the double doors that permit access into the main corridor.

All doors must be closed before a successful scan will allow one of the three doors to be opened. As before, an Iris Scan and a badge are required to enter the main corridor.

SECURITY CAMERAS



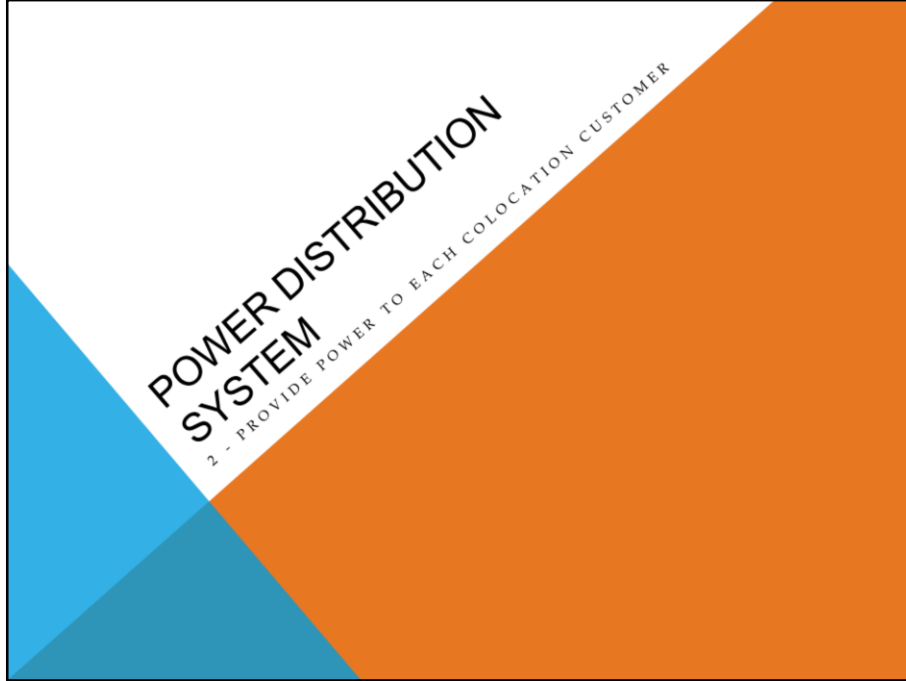
We have cameras at critical access points into and out of the building. We also have coverage for each aisle or racks.

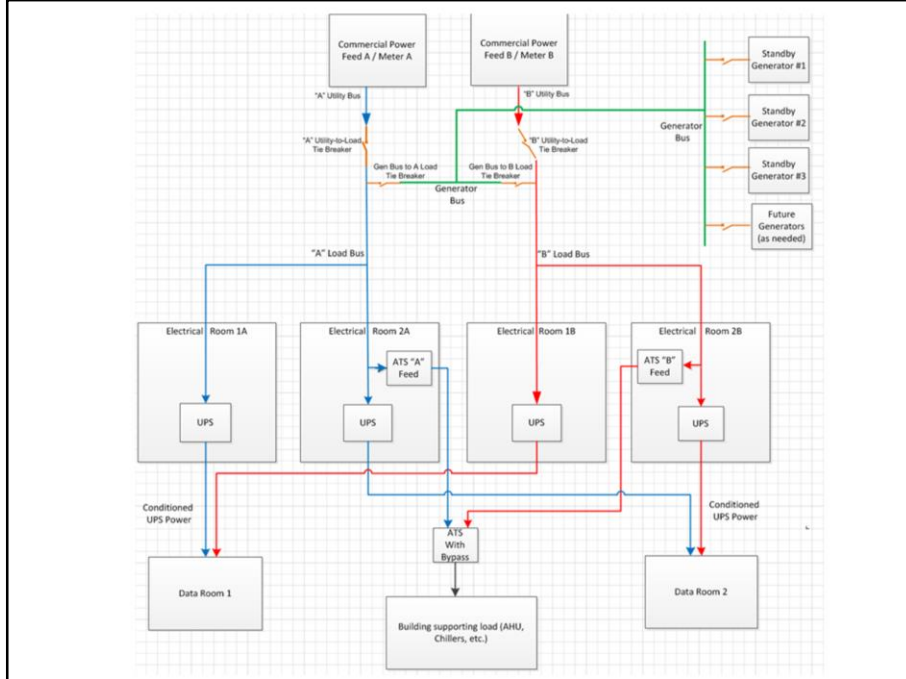
We save camera data per a defined data retention period

Remember, these are a deterrent and a forensic control – not a preventive control



Cameras are monitored at the reception desk, in the facility command center, and at another remote data center





Here is a One Line Power Distribution Diagram that illustrates the physically isolated electrical equipment rooms with separate active distribution paths

We have 2 utility feeds coming from two separate sub stations (Same power company though)

The power feeds come into separate sides of our building. An entire data room can be run from a single electrical room.

(generators)

EMERGENCY STANDBY GENERATORS



N+1 Generator Configuration

The Tier 3 Requirement is 12 hours of fuel on hand. We keep 30 hours of fuel at full load with redundant refueling contracts.

We call for a truck when the generator kicks on and it is not a test

We test each generator under full load every month

{Story about the CIO & the Combine} --Design to a specific level of protection

ELECTRICAL POWER ROOMS

- Each data room is fed power from (2) different electrical rooms.
- Each electrical room is internally redundant (2 UPS systems, never to exceed 40% load)
- Each electrical room is externally redundant (one room can sustain the entire data room)



POWER DISTRIBUTION PANELS

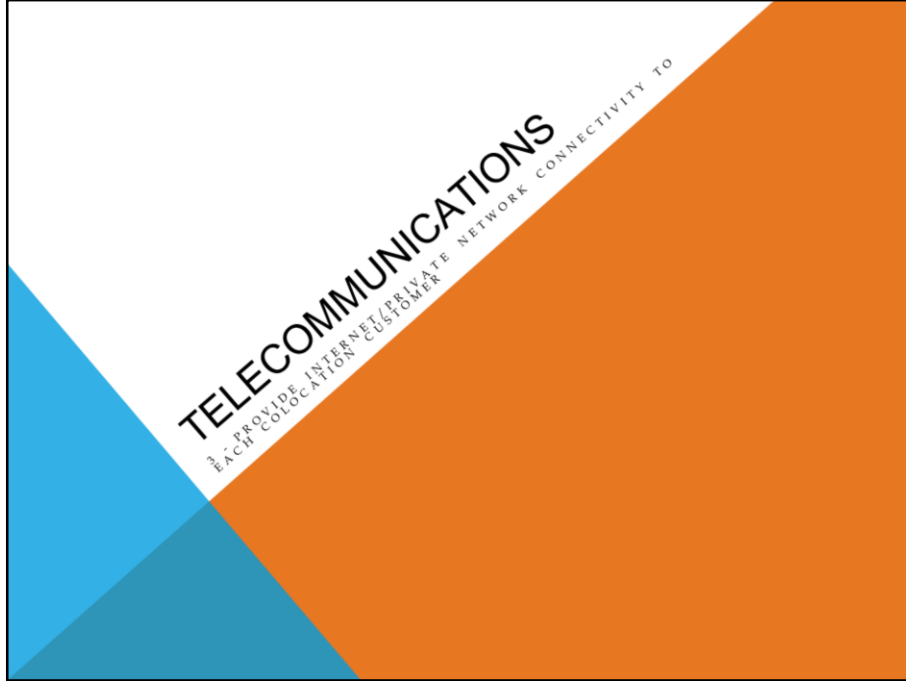


In each data room, every row of racks has 2 PDU's (power distribution units) for A and B side power to EACH rack.

The power draw is measured by our building automation system at each breaker in the power distribution panel and customer's are expected to ensure that the load is balanced across the A & B side (as you would expect if they are using equipment with dual power supplies)

Since we design each rack to draw up to **5kw**, this means that we can supply **160 racks** in each data room

And our electrical distribution has been designed to have fully redundant capacity at full load



MULTIPLE TELECOM CONNECTIONS						
	Cedar Falls	Des Moines	Minneapolis	Madison	Phoenix 1	Phoenix 2
Telecom						
Telco Entrances	Three	Two	Three	Four	Two	Three
Telecom Carrier						
	AT&T Cedar Falls Utilities ICN, IINS Mediacom Paetec Centurylink Sprint Verizon	CenturyLink Fiber Utilities Enventis Windstream Mediacom NexGen	Centurylink Comcast Enventis TDS Telecom tw telecom Zayo	AT&T Charter TDS Telecom WIN	CenturyLink Cox TDS Telecom	AT&T Global Crossing CenturyLink Cox OneNeck
Internet Providers						
	Centurylink Cogent	Centurylink Cogent	Cogent Global Crossing	Centurylink OneNeck IT Solutions		

High network availability is achieved by supporting multiple carriers and Internet providers and offering blended Internet to the customer at a particular SLA

We have all heard the horror stories of a backhoe taking out network service. Situations like this are mitigated by having multiple Telco entrances at opposite corners of the building.

At our purpose built facilities, the fiber vaults are close to the building (as opposed to the edge of the property), they are locked, alarmed, and under a CCTV camera.



RACKS



- **Chatsworth GlobalFrame**
- **CPI Passive Cooling® Solution**
- **Perforated front doors**
- **Solid side panels**
- **Internal Power Plugs**

Thermal management is one of the greatest challenges in a data center.

The Rack solution that we use helps us use the cold air we have more effectively by directing it through equipment where it is needed most.

Our design now has the power plugs inside the cabinet. In the past, we did it like everyone else and suspended the rack power plugs above the cabinet.

Then we invested in a lockable, tamper-resistant cover for the plugs. Until someone came up with the elegant idea of running the power cable into the cabinet and keeping the plug inside the locked rack.

{Elaborate solutions occur first, and then elegant ones}

CUSTOM CHIMNEYS



We use a custom designed chimney to evacuate the heat out of the top of the cabinet, drawing in air through the perforations in the rack's front door

Sometimes people will remark at the relatively warm temperature in the data rooms (72-74 degrees). We are able to achieve this because of this airflow design and we are not wasting energy cooling anymore than necessary

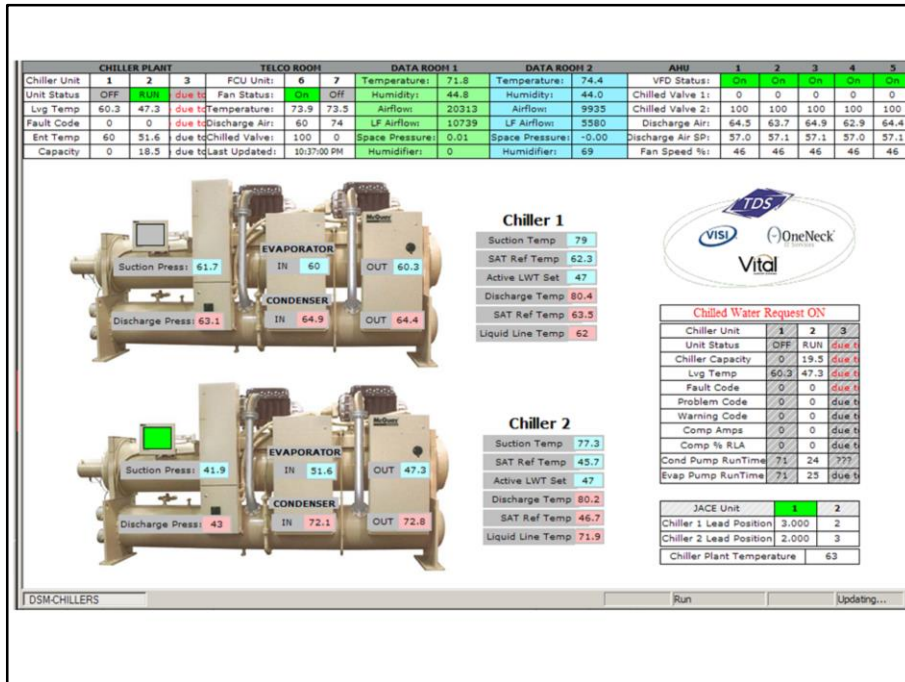
CONDENSERS



Hot air exhaust is transferred to the water pipes in large fan units that draw the air through the racks.

The cooling water pipes go to a series of chillers, which transfer the heat they take out of the water and return to the fan units.

This picture shows the evaporative cooling tower units outside (effectively a large radiator) water is sprayed over it,



We have Three 275 ton centrifugal chillers and One 550 ton chiller in Madison

Again, everything is monitored by our BAMS



We have massive water softeners in order to condition the “spray” water to preserve the cooling towers’ exterior surface and piping.

This prevents corrosion, extends the life of the pipes and reduces maintenance.

The cooling is based on a redundant closed loop system of pipes for all critical piping and all redundant equipment can be bypassed for maintenance while the DC is in full operation.



FIRE SUPPRESSION



Like many data centers, we use a dry gas fire suppression system.

- Liquid-based fire suppression systems can cause major damage to – and even destroy – the very things they are supposed to protect.
- Instead we use either FM 200 or FE25.
- These fire suppression systems deploy quickly and cleanly and won't leave behind oily residue, particulate, or water.
- FM-200® systems reach extinguishing levels in 10 seconds or less, stopping ordinary combustible, electrical, or flammable liquid fires before they cause significant damage.
- Approx cost of a large FM 200 tank is \$55,000. Obviously, we want to avoid that expense and the disruptiveness of a discharge...

VESDA



Very Early Smoke Detection Apparatus

So in addition to traditional smoke detectors, we use a VESDA system:

This is an active system (as opposed to a passive system like a normal smoke detector) which takes continuous samples and is able to distinguish between dust particles and smoke particles. It is also about 1000 times more sensitive than your home system.

Interesting Fact – the way that they demo the VESDA systems is to take a toaster, drop in a circuit board and hit “toast.” Before there is any significant smoke, the VESDA system will alarm.

BUSINESS IMPACT ANALYSIS

KEY ACTIVITIES THAT SUPPORT COLOCATION

- Control Physical Access to Colocation Customer Equipment
- Provide Power to each Colocation Customer
- Provide Internet/Private Network Connectivity to each Colocation Customer
- Provide Controlled Temperature & Humidity to the Colocation Data Rooms
- Provide Fire Protection to the Data Room



"Hedgehog Concept"

Control Physical Access
Provide Power
Provide Network Connectivity
Environmental Controls
Fire Protection

SUMMARY

- **Controls & Control Objectives**
- **Use Policy to Create a Mandate**
- **Defense in Depth for Key Activities**
- **Key Activities from BCP**

*That which is worth doing
...is worth doing well*