Securities Essentials Course - Practical Submission 1.2f

Requirements for the Design of a Secure Data Center

Philosophy

Physical security is a crucial part of the system defense matrix. Events of recent months a have served as a catalyst to look at data centers with an even more critical eye. Most companies do not have the luxury, or the financial depth, to locate data centers hundreds of feet below granite mountains with complete cities to support them. Proper planning and design will allow you to construct a facility that will be secure, defendable and cost effective. Some may read this and say that it is ridiculous to even consider some of the items suggested as possible threats. The biggest threat is the thing you don't consider. Every potential danger must be at least noted and the cost to protect against it evaluated. It can then be incorporated into the facility design with multiple layers of security, or discarded. Remember to plan for the worst and hope for the best.

I. Site Selection

The neighborhood where the facility will be located should be chosen carefully to get the best mix of ideal features. The site should be in a safe area that is not subject to any natural environmental dangers such as flood planes or an area subject to landslides. Earthquakes are possible in most every part of the country but if you are forced to build in a seismically insecure area the structure can be hardened accordingly. Have soil borings taken before purchasing your site. Soil borings are vertical samples of the ground that are then analyzed and test to determine makeup and bearing capacity. The depth of the boring will depend on the type of materials found. They are generally drilled until stable material is found. If the history of a site is in question check not only for stable soils but possible ground contamination from previous owners.

Make sure the site has adequate drainage. Even if it not in the flood plane verify that there is good drainage and runoff paths so localized flooding will not occur during heavy rains or snow melts. If your facility will have below grade spaces make sure that a perk test (measure of absorption of water into the soil) is conducted. Sub-grade spaces should also include a water tight design, i.e.., a pool that keeps water out. This goes beyond the typical damp proofing applied to basements. If your building is subject to a sustained period of heavy rain or localized flooding there should be enough resistance to water penetration that you do not have to depend on sump pumps to keep dry. Your whole facility might be running on generators and it is better to have the power for systems instead of basic building functions such as pumping water from you basement. Also remember the deeper your facility is in the ground the higher the hydrostatic pressure (force of water in the soil against the walls) will be and the greater chance of leaks.

The secure data center should be constructed in a quiet area with low surface traffic, but at the same time it should have multiple access roads into the area. It should be innocuous and unassuming. Other locations to avoid are banks (crime targets), parade routes (block access to facility), chemical plants, sports arenas (anything that generates large amounts of street or foot traffic). Attempt to locate in areas with stable weather patterns. Hurricanes and tornadoes can not only impact your facility but also the overall area's utilities, services and traffic patterns which will affect data center operations. It would be unwise to locate the center in an unstable neighborhood that is subject to gang activities or high crime. The events of September 2000 have shown it is just as unwise to locate near prominent sites that can be seen as political focus points.

In addition to the terrestrial dangers do not forget about airborne problems. The flight paths for airports are often where inexpensive land can be found. Although your accountants may think it is a great place to construct a facility, it is not a safe location. Airplanes can crash and it is often during takeoff or landing. Also it is really not that uncommon for planes to loose parts while taking off. Planes taking off have lost tires, engines and other parts. A large object such as a tire or engine would have a devastating effect on any building they might hit.

Talk to you new (or existing) neighbors. Develop plans with neighboring businesses that address reactions to possible events. Ask them to call if they see any irregular activity on or near your site. They can also let you know if they hear of any upcoming events such as area construction etc, that could potentially affect you operations. Equipment operators are notorious for cutting underground cables even when they are marked.

II. Utilities

A good site location will be near available fiber from multiple providers and redundant power grids. It will be less likely that you have to rely on backup generators if you facility is drawing power from multiple grids. If you have the option of selecting where your facility will be located, look at the historical data for the local power providers. They are not all created equal.

Fiber access will be more dependable and cost effective if you have options from multiple providers. Internal facility routers should be able to manage traffic and automatically switch to the best path.

Look for close municipal services such as police and fire. Hopefully you will never need them but if you do response time is critical. Also take a moment to look for the comfort level of your staff. Although not a direct security concern, a good selection of nearby restaurants can keep your staff happy and reduce travel time on breaks which will help keep them alert.

III. Building Design

The building should be located at the center of your site with clear unobstructed views on all sides. An extremely critical installation might be fenced. Even if your facility is not in danger from someone physically attacking it, a perimeter fence can reduce the chance of random vandalism. (Note: key public infrastructure facilities such as utilities and MAEs should be designed in a manner that assumes an actual attack will occur.

You do not want to advertise the nature of you facility. A false name on a building sign can also help camouflage the operation. Pick a boring name such as “Standard Paper Products”. Just make sure you don’t pick the name of a real company that exists in you area.

Design of the data center must be based on durable materials that can exceed normal design loads. At a minimum the facility must be capable of withstanding 200 mile per hour winds and driven rain or snow. Studies are currently being conducted to develop tornado resistant structures. Developments in this area should be closely watched by companies doing business in areas of the country susceptible to these storms. Material such as masonry and concrete will afford the most protection to your facility along with fire resistance. Include only necessary windows in the structure. Make sure that you have 20 foot high ceiling for tolerance of over temperature conditions.

Driven rain and snow are a capable of penetrating your facility and damaging equipment. Most properly constructed walls will resist this infiltration, however vents and intakes should be carefully selected to make sure they can channel away any water that does get in. Pay particular attention to this item since many louvers that claim water resistance will not offer protection in high winds. Buffer zones must be provided behind these eternal openings where any moisture that penetrates can be safely removed. Remember the more air you have to bring in for heating and cooling the larger these openings become. It is important to remember that the air you bring into the building should also be adequately filtered to keep contaminants out of the facility. The structure should be tight to ensure high winds do not contaminate the spaces with airborne dust and dirt.

Roofs and materials should be carefully selected and designed to resist not only water but winds, ponding (the build up of water on flat roofs), snow loads and uplift (negative pressure exerted by a roof in high winds). Uplift combined with a poor edge detail can allow the entire roof to be ripped off in high winds. The roof should withstand at least 200mph winds, however spacial conditions caused by your geographic location may require higher design loads,

Generally due to cost factors facilities will have flat roofs with either a built-up or membrane waterproofing. Make sure that if your facilities roof is flat that it is adequately drained and includes relief for ponding if the drains become plugged. Provide overflow scuppers to prevent ponding that could collapse the roof or cause leaking. In all designs make sure that there are multiple drainage paths for all roof areas should one become clogged. Never have a design that traps water.

IV. Mechanical/Electrical Systems

As noted earlier the data center would be best with dual electrical service feeds and distribution from different power grid sub-stations. Protect your equipment with power conditioning for surges, sags, high energy transients, brownouts and blackouts, regardless of the source of the electrical disturbance. The electrical power design must isolate end point distribution to address harmonic loads and surges caused by internal equipment also.

Make sure to avoid ground loops in you power design. This can happen if you tie the grounds for building equipment and computers together. Surges from equipment startup can back feed on the ground wire leg and damage sensitive gear such as computers. Isolate computers from heavy equipment such as air handlers by using separate ground rods (ground rods are metal rods that driven into the earth to provide a permanent earth grounds to route surges) that are located at least 6 feet apart. (1)

The dual feeds should pass through redundant automatic generator systems with individual capacity for entire facility; including building systems such as heating, cooling lights and security systems. Primary generators are usually diesel fuel units or natural gas. Both have weaknesses. Diesel fuel can run dry and the tanks require environmental spill containment. The fuel must be stabilized for long term storage and can run out during a prolonged outage. Natural gas generators can be affected by geological events or damage to the distribution system facilities. Diesel generators with a minimum of 5 days of fuel provide the most self sufficient design. (If the facility is strategic in nature consider installing multiple generators which run on different fuels, two diesel and one gas generator, or vice versa depending on your fuel selection). The power should automatically switch over to generators during an outage. Critical systems would then be attached to dual Uninterruptible Power Supplies (UPS) systems to insure that they are unaffected during the generator startup period.. These power systems should be modular in design and allow for hot swapping of all components. Monthly tests should be conducted to ensure status of equipment. Provide maintenance bypass around normal distribution to critical loads.

Computer rooms have many different pieces of electrical equipment being used. Provide an access floor to create an interstitial holding place for the cords and cables required by the systems. (An access floor is actually a floor raised above another floor). Access floors are constructed of 24 inch by 24 inch panels on a frame. The panels are interchangeable and allow wire and cable changes without disrupting center operations. This space can also provide a method of distributing conditioned air to workstations above the floor through diffusers (or vents) placed throughout the access floor. All equipment areas should have 18" to 24" raised floors and open data trays for flexibility and quick access in emergencies.

Provide dual cooling and heating systems utilizing down flow discharge modular cooling units for most effective systems. (However bottom discharge, floor mounted, water etc may better suit your individual needs). Design to maintain consistent temperature and humidity to counteract the hot dry air created by you equipment. Remember that equipment density is constantly rising and along with it the heat and energy loads. Ensure that you have adequate capacity for the future power and HVAC needs of your facility. Provide for potential future expansion without disrupting the business operations. Any disruption of the existing equipment during a renovation creates the chance for an unscheduled outage and or data loss. All environmental controls should be monitored with logging, trend projection and alarm notification. Remember that location of equipment is as critical as the type. Provide easy but secure access for maintenance. Also include the capability in facility design to replace all pieces of equipment without effecting operation of the facility.

Fire is also an unfortunate danger in a data center. Since water and computers don't mix, it's important to have a fire-suppression system that's designed for computer rooms. Installing halon systems and refilling halon tanks is now illegal in the United States. FM 200 is the new industry standard replacement for halon. It can be dispensed within 10 seconds or less and does not leave behind any residue or particulates. It is people, equipment and ozone safe. Existing halon system, can be converted to an FM 200 system. It will require little more than changing the tanks used in the current system. It is possible that local fire codes will require that you have a sprinkler system, even if you also have an FM 200 system in place. If this is the case, make sure that the sprinkler system installed in your data center is pre-action; meaning that the pipes are normally filled with pressurized air-and that the sprinklers are meant to go off as individual heads rather than in zones, or over the entire area. Make sure there's adequate drainage available for both the FM 200 system and the sprinkler system, in the event that they are needed.

V. Facility Security / Monitoring

In addition to the monitoring of environmental systems, the data center should be equipped with multiple security systems. Passage into and out of the facility should be controlled by card or biometric access systems. All security systems should be monitored 24/7 and activities logged both onsite and at a remote location. All alarms should specify the exact location of the fault so time is not wasted searching for the source of the problem. Motion sensors, CCTV systems monitoring both the interior and exterior should be equipped to handle low light conditions. Only staff members should be allowed unescorted access in the facility. The staff should only have access to areas that are required by their particular duties. Make sure that all visitors appointments are verified before allowing escorted access only to the necessary location. The security monitoring equipment and staff should be in a highly secure area separate from the main computer equipment. Make sure critical screens can not be viewed by passers by or through windows.

To protect against fire install a very early smoke detection apparatus (VESDA). By detecting any possible fire before it has a change to erupt into a major event you can contain and hopefully extinguish it before it impacts the overall operations of your facility.

The following is a suggested list or items to monitor and provide notification to staff in the event of alarm:

Intrusion
Fire
AC Power failure
High/Low voltage alarm
Generator failure
UPS Failure
Temperature/Humidity
Breaker Trips
Leak Detection
Underfloor water detection

VI. Construction Monitoring

Monitoring and access control to your facility should start in the early stages of construction before foundations are even excavated. This is crucial in government or military facilities, but also in critical business or infrastructure sites. A prime example of danger in the lack of oversight was demonstrated by the United States government facility constructed in Russia during the cold war days. The walls and concrete had numerous bugging devices care of the local labor force and the KGB.

As the world has seen the fall of political barriers there has been a rise in the global face of business. Corporate espionage has taken on a nationalistic flavor as some countries have been rumored to have turned their intelligence communities into business research groups, i.e., they are now investigated your company to see what they can learn to help business at home.

Make sure that all construction is monitored and that the site is completely secured at night. If you feel at risk, have the building swept at various stages of construction for any devices that might have been implanted.

VII. Electromagnetic Pulses (EMP)

If someone were to have suggested the need to worry about electromagnetic pulses a year ago they would have been looked at as if they were insane. Unfortunately there are insane people loose in the world so every possibility no matter how remote should be at least considered, especially if your facilities services are critical. "The EMP from a single hydrogen bomb exploded 300 kilometers over the heart of the United States could set up electrical field 50 kV/m strong over nearly all of North America"(2). Devices detonated at lower levels, such as from an aircraft would impact a smaller area but with much greater impact.

Regarding the cost to harden a facility, in 1997 Dr. George W. Ullrich Deputy Director Defense Special Weapons Agency stated; "if provided for at an early stage in system design and development. For a tactical system, the cost can be as little as 1% of the total development investment; for strategic systems, a target of 5% is reasonable. Retrofitting protection after a system has been deployed can be considerably more expensive."

VIII. General Issues

The following general issues that should not be overlooked in the facility design are both practical and operational.

Utilize experienced qualified professions in the design and construction of you structure. Your facility is not the place for them to learn how to do it. Get references and check them.

The design team must make sure that all applicable codes are conformed with. Make sure that this includes handicapped accessibility.

Have the team analyze the use of the facility. If there will be different groups or departments working withing the secure areas, attempt to physically separate the different groups to enhance security. This might be separating the accounting group server from research and development's. Or if you are hosting equipment for different users isolate each groups equipment and develop a security method that is easy to both administer and use.

Look at both one and two story facilities when planning the design. There are benefits to both. While strictly speaking either can be secured, depending on you needs one might work better than the other for you and there are different architectural benefits and costs to each.

Do it right the first time. It will be extremely difficult to make changes once your data center is in operation.

Make sure backup tapes are stored at a separate remote facility. Security offsite must be at least as strong as that at your data center. If storage must be maintained on site it should be in a fire, flood, bomb proof vault. Even then this is not a good idea.

Do not make public any information about your operations. This includes but is not limited to location, staff, design or security features, type of equipment, etc. The smallest pieces of information can be used to compromise security.

IX. Cleaning

The data center must be kept free of dust and dirt. Incorporate the ease of cleaning into the facility design so all areas can be reached. Provide for needs of cleaning crews such as power and water, (I have seen a cleaning person reach for a system plug to remove because there were not free ones readily available). Try to eliminate any airborne or tracked dirt by building systems such as filters and drained walk off mats at entrances. Utilize antistatic materials on surfaces wherever possible. Building ventilation system should be designed in such a way that filers can be easily reached and changed. Generally rooftop units are cheaper to install but often fail because they do not allow easy maintenance.

Do not keep paper or other flammable material near equipment. Make sure that they are stored in a fire resistive construction.

X. Planning for the worst

Include hotel facilities, that is sleeping and eating accommodations for those emergency situations where your staff may be confined to the facility either by weather, social unrest of environmental contamination.

Have adequate food and water on hand to feed the typical staff for at least two weeks. Meals Ready to Eat (MRE) are available for hiking/camping, are available in 2-week kits and are safe for long term storage. These meals don't require cooking or heated water. They are ready to eat straight out of the pouch. If you have an onsite kitchen that is routinely used you can have more interesting food choices of food. You might still prefer to keep items that more easily or quickly prepared.

REFERENCES

1. Email newsletter December 2000. Steven W. Piel Sr. Service coordinator/project management, Data Impressions, Inc. / South, Gate, CA mail to:steven@dataimpressions.com

2. "Mushrooming Vulnerability to EMP," Aerospace America, August, 1984, p.74.

http://www.alcatexinc.com/fire.html
http://eb-datacenters.com/dtf.html

http://www.dcdonline.com/siteprepnew.htm

http://www.saveinc.com/guidelin.html

http://internet.about.com/cs/datacenterdesign