

The Data Center Defense Dossier

By Steven Harris, Forsythe

In a world where every IT director and security expert gets his wish, data centers would be constructed with dual electric power feeds, multiple generators, redundant heating, ventilation, air conditioning (HVAC), dual-interlock dry-pipe fire suppression systems, iris scans, laser grids, man traps, face-recognition devices, and a surfeit of other technologically advanced systems and procedures. In the real world, operating costs and business strategy intercede, and companies must develop the most practical and effective methods for building and securing their organizations' mission-critical data centers.

Rather than one universal set of best practices, there are good and better practices that best fit the needs of an individual organization, including the organization's size, mission, budget, client base, and strategic business objectives. When determining what data center practices best fit each organization's current and future needs, location and physical security are two critical areas that must be considered in light of, and sometimes weighed against, overall business requirements.

Location, Location, Location

In determining the location of the data center, the first step is choosing a site within a localized geography that meets the overall business objectives as well as conforming to a good or better practice. From a risk standpoint, an urban downtown area, replete with high rises, heavy vehicular and foot traffic, government agencies, and corporate flagship buildings, may not be the best location. Putting a data center in a downtown high-rise building represents a significant risk in terms of both safety and cost. It is less expensive and, in general, more secure to develop data centers in low-rise suburban buildings or business parks within an hour's drive from the city center. However, the availability of telecommunications and power is typically greater within major city centers.

Accessibility is also an important business consideration. The cachet of having a certain address is another business driver that sometimes influences a data center's location. When choosing a location it becomes important to strike a balance between distance from an urban center (to reduce

exposure) and proximity (to maintain infrastructure efficacy and ease of doing business).

There are also several common-sense factors to consider when choosing or building a data center. For example, because of the risk of flooding, rivers, streams, and lakes should be avoided when selecting a site. In the event of a flood, even if the data center remains dry, it may be difficult or impossible to reach the building. Better practices for locating a data center also include:

- Avoiding airport flight paths
- Observing proximity to electrical substations, overhead high-tension electrical power lines, interstates, rail-lines, etc.
- Assessing prospective neighbors to avoid hazardous manufacturing or distribution facilities and other unwanted security threats

In other words, disaster avoidance is the baseline. Another aspect of location is determining where the data center should reside within a building. Creating a "building within a building" is an effective method for isolating the data center inside the building and keeping it off the window lines, thereby reducing the likelihood of external penetration. The closer the data center is to the center of the building—away from the basement, the roof, and the outer skin of the building—the safer it will be.

Sometimes organizations have the option of constructing their own data center. In these instances, broader questions arise, such as: How far should management go to protect its assets? For example, the more business functions that exist beyond the data center within the building, the greater the likelihood that something will go wrong. Many employees in a multi-function building may not even be aware there is a mission-critical space in the building. As a result, they may not take the extra security and safety precautions required to better protect the data center. Therefore, to achieve the highest level of security, a company could construct an IT-only building with no other business functionality on site. However, management must balance the requirements of the data center against the overall business needs.

Physical Security and Human Access

In contemplating the physical security of a data center, the objective is to allow the right people to gain access, while keeping the wrong people out. This realm of data center security can begin with something as simple as a card key, a proximity badge, or a cipher-lock, which is a key pad that requires the user to enter a multi-digit numeric code. At the top of the line are biometric security systems, which can include, but not limited to, handprint recognition, iris scans, and face recognition. These tools can be combined with other elements of physical security, such as a single-person man trap with weight calculations that determine whether or not the individual is carrying something in or out of the building. Cameras and their associated recording devices are an integral part of the security system for most data centers. They come in many varieties, including fixed or pan/tilt/zoom; black-and-white or color; continuous action or motion-sensitive; still photograph or full motion; spot or blanket coverage. A wide range of combinations of security systems and devices can create a highly restrictive barrier for people trying to access a company's property, its buildings, and its data center.

The company's business needs, capital spending guidelines, the demands of its clients, and relevant federal regulations will dictate the level and type(s) of physical security it implements. When determining which good and better practices fit your organization, a balance must be struck between two extremes: absolute security and ease of doing business. In order to do this, the right questions need to be asked: How has our business changed since the data center's physical infrastructure was built or last remodeled? What data center issues or problems are we currently facing or anticipating? What new business drivers or client requirements do we need to consider? What new regulations are we facing? What level of compliance do we feel comfortable achieving? Is this capital spending intended as a short-term band-aid or a long-term design change?

For most data centers, as the business grows and attracts bigger clients, the corresponding risks and expectations also increase. The needs of your organization today will likely not be the same in three, five, or seven years. However, most data centers are designed and built to last for many years. Thus, the base infrastructure should adhere to as many good or better practices as possible. And, just as you replace and refresh your IT environment from time to time, so should you continue to migrate to better data center practices, keeping in mind that "better" means what is better (or best) for a particular organization. In data center development and security, there is no one size that fits all.

Published in Next-Gen Data Center Forum, February 1, 2005.

As director of data center planning for Forsythe, Steven Harris helps clients with data center planning and design issues including facility assessment and optimization, floor plan design, site selection, disaster recovery planning, and project management.

