WEST 7 CENTER

How Secure Is Your Data?

Underground Data Centers Provide the Ultimate in Physical Security, But Not All Are Created Equal

RISING JLL

Contents

Protecting Critical Data from Virtual and Physical Assault

According to IDG's 2017 U.S. State of Cybercrime report, an annual survey conducted in partnership with the U.S. Secret Service and Carnegie Mellon University, the average IT security budget across all industries and the public sector is $11 million. This should come as no surprise, given a prediction by Cybersecurity Ventures, a leading researcher for the global cyber economy, that cybercrime could cost the world $6 trillion annually by 2021, doubling from $3 trillion just three years ago. If correct, this would represent the greatest plundering of economic wealth in history, while discouraging the business incentives for future technology innovation and investment.

While it's understandable that data center providers and their customers place great emphasis on cybersecurity, physical security within the data center is too often an afterthought. Notwithstanding the ongoing enterprise migration to cloud-based infrastructure, data centers are still the substantive fortification protecting critical data from both virtual and physical assault. While technology companies and media tend to talk about the cloud as if it existed in some ethereal realm, the fact remains that much of the actual hardware used by the major public cloud providers in the U.S. resides in colocation facilities alongside servers used by other companies.

Moreover, while ensuring the physical security of cloud servers is essential, so is safeguarding mission-critical business applications, content, data storage, networking and computing related to Big Data analytics and emerging technologies such as artificial intelligence (AI), machine learning and IoT-enabled devices. Additionally, if a data center houses information related to financial records or other regulated industries, there are statutory requirements pertaining to physical security that are non-negotiable.

> “...cybercrime could cost the world $6 trillion annually by 2021.”

Bad Actors, Off-Script

Even if cybersecurity measures are in place, there are many ways that bad actors can physically threaten a data center. For this reason, the best way to protect a data center is by implementing strong physical security measures that are complementary to cybersecurity protections.

If you're skeptical about the penetrability of data centers, then consider the case of a Chicago-based colocation facility that was the victim of not one, but at least four physical security breaches over the course of two years, including burglaries and robberies. According to police reports, in one incident, data center customers lost hundreds of thousands of dollars in computer hardware, as well as access to sensitive data when a security guard was robbed of his biometric reader, allowing assailants to enter the facility. Another breach occurred when intruders used a chainsaw to enter through a wall.

And then there was the physical breach that took place in 2011 at Vodafone's data center in Basingstoke, England, approximately 50 miles southwest of London. A band of marauders broke in and made away with servers and networking equipment. Vodafone's systems went down, and the telecom company's business reputation suffered greatly in the aftermath.

Although most data centers implement extensive measures to secure the perimeter of a facility, a report by IBM Research Data found that 45 percent of breaches occur as a result of unauthorized access. So, let's examine the best practices of sound physical security at the data center.

Physical Security Best Practices

As discussed, a physical breach of a data center could lead to a server or rack being stolen, damaged or incapacitated, which could also mean that sensitive data might become temporarily unavailable or irretrievably lost, depending on backup resources. While some data center managers may underplay basic physical security measures because they assume that theft is unusual, the likelihood remains that anything that isn't locked up can and will be stolen. For the simple reason that criminal enterprise is generally not known for its application of risk-reward analysis, that includes the three-year old $10,000 storage area network server that's worth only $50 at the local scrap metal yard.

Today, however, given advances in technology, the present geopolitical climate and the specter of domestic terrorism, physical threats have the potential to become much more sophisticated. As the late Uptime Institute founder Kenneth Brill has written, “Previously in the realm of science fiction, asymmetrical physical attacks on data centers by explosives, biological agents, electromagnetic pulse, electric utility, or other means are now credible.”

Data centers can effectively tackle most issues of physical security by planning and implementing the right security measures. The most fortified data centers deploy multi-layered security access methods including visual inspections from multiple 24x7 guard stations and video monitoring, and biometric access controls and keypads. Best practices also incorporate double-locking mantraps at the data center entrance and restrictive access policies for each customer's space, providing security within each zone of the facility. Even so, there are other foundational measures to data center security.

Power, the Cornerstone of Data Security

While ransomware and Distributed Denial of Service (DDoS) attacks debilitating and breaching the security of entire networks may garner most of the headlines, a recent survey by the Uptime Institute found that the leading cause of data center failures (33%) are power outages. For this reason, organizations including Cloud Service Providers (CSPs), Over-the-Top (OTT) content and Content Delivery Network (CDN) providers that opt to partner with a data center that addresses issues involving power make one of the best decisions they can with respect to data security.

33% of data center failures are power outages.

The Uptime Institute, for example, classifies data centers as Tier I, II, III or IV, based on their infrastructure capacity, system availability, redundancy and concurrent maintainability. The Tier III classification indicates a highly reliable facility with fully redundant critical power distribution system and cooling components. Tier III data centers can lose an uninterruptible power supply (UPS) or generator power and still maintain operations. Equally important, a Tier III facility allows data center operators to perform regular maintenance on power equipment and regularly test capacity and failover without interrupting ongoing operations. Many data center failures that can be traced to UPSs and generators are simply the result of unmaintained equipment. Hence, testing and maintaining power hardware is an effective way to keep things running smoothly. Data security is therefore directly related to maintaining data center operations and staying online.

Location Is Key

Another critical decision that CTOs, CIOs and CSOs make about data security is where their organization's data and mission-critical applications are stored. McAfee, the global computer security software company, once published a survey of more than 800 C-suite leaders from varying industry sectors. The report revealed that 50 percent of the respondents stated that they would like to move their data to a more secure location. Moreover, 74 percent believed that selecting a secure data center would provide them a competitive advantage in the marketplace.

Where security and data center location are concerned, a critical criterion is the region's risk of natural and man-made disasters and the facility's ability to withstand such an event. Data centers located in areas that are especially prone to hurricanes, tornadoes, flooding, or which are not constructed to withstand seismic disturbances are especially vulnerable. A clear example is 2012's Hurricane Sandy whose severe flooding forced many New York data centers offline for several days, resulting in significant recovery costs. When we consider a Federal Emergency Management Agency (FEMA) report that found more than 40 percent of businesses never reopen after a disaster, the question of physical security in relation to data center location can no longer be ignored.

But aren't all data centers at some level vulnerable to extreme weather, intruders or sabotage? The answer is that some data centers and colocation facilities, by virtue of purpose-built underground design, provide a superior bulwark against even the most formidable man-made and natural threats.

Underground, But on the Coast

Underground data centers can be found in Lithuania, the Netherlands, Norway, Switzerland, Ukraine, the United Kingdom, and Sweden, as well as the U.S. While data center operators have been retrofitting underground Cold War era defense bunkers and mining operations sites into data centers for many years, there's an increasing interest in subterranean facilities to host mission-critical applications, cloud servers and sensitive data as concerns about security and energy as well about terrorism have come to fore.

Underground data centers feature several significant advantages as compared to their above-ground counterparts. Most notably, subterranean data centers offer the ultimate in physical security and resilience, protected as they are from extreme weather events such as hurricanes and tornadoes, or the approach of unauthorized intruders. In regions where earthquakes are of concern, structural reinforcements that exceed seismic performance standards provide resilience that's still superior to older structures that could collapse during a major earthquake. Additionally, the speed with which an underground data center can expand its capacity is improved since construction can take place year-round regardless of weather conditions. Finally, underground facilities are naturally cooler, which can reduce power usage.

Still, not all underground data centers are created, or located, equally. As with above-ground facilities, the geographic location of an underground data center or colocation site is a critical touchstone for prospective CSPs, OTT players, CDNs and other organizations to consider. Most U.S. underground data centers are clustered in the Mid-West, many of which are housed in former limestone mines. For these subterranean data centers, remote from major metro areas, the cost to bring in power and installing fiber-optic and high-speed network connections could be prohibitive. Remote underground facilities are also problematic in disaster recovery scenarios brought about by extreme weather events, when travel to a data center further away can become virtually impossible.

By contrast, the underground data center that is sited in a major metro area does not face connectivity challenges because such a facility is in proximity to the existing information technology environments of customers, and providers can easily run fiber connections to other network transit points in the city. And if that underground data center happens to be located in a coastal city such as Los Angeles — a global business hub where many international carriers and internet providers have points of presence (PoPs) — then customers have access to high-speed networks and subsea cables providing connections to international markets across the Pacific, expanding their business opportunities.

.

WEST 7 CENTER

West 7 Center: The Secure, Underground Data Center Providing the Gateway to the Asia-Pacific

Located in downtown Los Angeles, West 7 Center is a secure and reliable facility with multiple options for connectivity. With three levels of underground data center space comprising 348,000 square feet, and 377,000 square feet across nine floors of above-ground office space, West 7 Center offers the ideal location for telecommunications companies, Cloud Service Providers (CSPs) Over-the-Top (OTT) content and Content Delivery Network (CDN) providers that require high performance infrastructure to run their operations.

The largest purpose-built data center in Los Angeles, a global business hub of four million people, West 7 Center also serves as the digital gateway to the Asian telecom market, enabling Asia-Pacific carriers and service providers to quickly establish a U.S. presence.

Contact us to learn more and schedule a tour of West 7 Center!

West 7 Center provides:

- **Underground data center offering the ultimate in security and protection against adverse events**
- **Total capacity of 22MW of power and 348,000 square feet of space**
- **13MW of generator power and 172,000 square feet of space available**
- **Carrier and cloud-neutral ultra-low latency connectivity**
- **Two central plants with N+1 uninterrupted power/cooling redundancy**
- **Three underground fuel tanks to support mission-critical operations in case of power outages**
- **Optimal location near residential areas and multiple IoT network edges**
- **Ability to provide custom-built facility**

Contact Info

Darren Eades
Executive Vice President
+1 213 239 6061
darren.eades@am.jll.com

Follow West 7 Center on social media for daily updates.

West7Center   West-7-Center