

File Created by [Blogging Rebirth](#) WP Plugin

## Colocation Security

In today's context of online businesses, the operative word is colocation. This is the setup where web hosting companies chose to colocate their hardware and infrastructure to third-party service providers.

One of the big reasons is to take advantage of the many advanced security measures the third-party service providers offer.

Because they collect a sizeable pool of income from their clients, colocation providers have invested top-of-the-line security hardware and technology for their system: physical protection of the servers and other equipments, safety of data and applications, and their protection from natural disasters like floods, fires, power failures and the like.

In choosing your colocation provider, you can take a look at these protection measures in these following areas for comparison purposes.

#### Redundant power sources

Nowadays, accidents and other devastations regarding power and power sources are unpredictable and can wreak havoc in a data center. Utility companies used to be dependable, but today's demand for power has grown so much faster than anybody can anticipate.

Today's colocation service providers have already incorporated the installation of backup generators that run longer. One generator is no longer viable given the unpredictability of public power sources.

What is more, they also have redundant generators that back up the primary units. Multiple power source alternatives are already today's industry standards.

#### Physical access security

Another critical area that colocation providers offer their clients is on-site security. Actively monitoring and controlling access to the building is a critical factor.

Truthfully, the only difference between you and Colocation experts is time. If you'll invest a little more time in reading, you'll be that much nearer to expert status when it comes to Colocation.

Aside from the must-have physical security measures, colocation providers now include biometric access systems. These systems generally include fingerprint and retina scanning for verification of people's identities.

So far, these modern sets of apparatus have been far more effective than the now-outdated key cards. (They were notorious for being easily stolen and duplicated.)

Other colocation providers have installed motion-activated surveillance cameras that can monitor activities outside and inside the facilities' premises. These cameras have been versatile enough to cover even the grounds surrounding the buildings.

#### Network access security

Normally, colocation clients are responsible in ensuring that their server hardware is protected with security software. On the other hand, colocation providers must also protect their clients from threats triggered by outside agents as well as from within the network itself.

One example is the now-debarred practice of one client cross-connecting their servers with the other tenants. The main reason is simple reduction of costs.

However, it also introduced a tremendous risk in the sense that if one client is compromised, the attacker is able to access the system of the other clients who had cross-connected for cost savings.

Many colocation providers have now forbidden this practice and had taken severe measures to make sure cross-connecting is not feasible or will not happen in their facilities.

#### Risk sharing

In colocation setups nowadays, both the provider and their customers are expected to share the ongoing common concern for security.

Compromising security is the greatest threat within this partnership. After all, it shall mean a total loss for the customer (sensitive data) and the colocation partner (confidence) where nobody wins.

#### About the Author

For all the latest articles and information on Investing In Silver please visit [Silver News Today](#)

You can also find this article published on [Colocation Security](#)