Stop Investing in an Inferior Data Center

Most private data centers lack the physical and virtual security measures of a 3rd party data center.

Alright, in all fairness, we've seen some well-constructed private data centers with excellent security, both physical and virtual. That stated, 90% of the private data centers we've seen could use a security overhaul.

Let's face it, a major security overhaul in a private data center is expensive. As IT leaders get to the line items in their capital and operational budget for data center maintenance and improvements, consideration of a third-party data center should be apparent, as cybersecurity is paramount in securing both corporate intellectual property and client data.

Any business that relies on data for its success – and let's face it, who doesn't? – has to make data security and system uptime a priority. And for those business owners who are trusted with their customer's data, such as patient records or credit card data, data security is at the top of their priority list.

But herein lies the challenge.

Owning and operating a secure data center requires advanced security measures that most in-house data centers are ill-equipped to provide. In addition, having the personnel, technology and processes in place to maintain a highly secure environment requires advanced technical capabilities and a substantial financial investment.

If you're one of the organizations that's facing these challenges of securing your data on-site, but know you're ill-equipped to meet each of the security measures your data requires, then maybe it's time to start thinking colocation. By working with the right colocation provider, you can be sure that you have security professionals on staff and the best virtual and physical security measures that today's colocation provider must provide.

Selecting a colocation provider with the proper security in place can significantly reduce your risk. There are a variety of measures that are implemented and maintained to help guarantee security and compliance within a third-party colocation facility including:

1. Physical Security – If physical security is top-of-mind for your organization, you're not alone. With a growing number of potential threats, both digital and physical, it's no wonder. Your valuable IT assets should be safeguarded against both man-made and natural disasters. Physical security measures should include security guards, video surveillance, mantraps, biometric readers and a physical process of ensuring a person physically checked the facility as specific times each day.

2. Network Security – The massive increase in malicious network traffic and the proliferation of SPAM have caused many businesses to be concerned about the security of their network. To safeguard your network, your colocation provider should provide IDS/IPS (intrusion detection services / intrusion prevention services) and basic firewall services. Additional optional services may include virtual firewall services, VPN services, content filtering, SPAM filtering, virus filtering, spyware removal, real-time traffic analysis using net flow reporting and real-time bandwidth reporting.

3. Compliance – As if IT departments didn't have enough to worry about these days, they also have to ensure that their organization is in compliance with various industry and federal regulations (PCI, HIPAA) which are designed to keep sensitive customer data safe. Your provider should provide as much assurance to their customers as possible, that their practices and methodologies are compliant with various compliance audit and certification requirements including:

- **Type 2 SSAE 16 (SOC 1) -** Validates that the providers organizational and information technology controls related to the services audited are fairly described, suitably designed and are operating effectively.
- **HIPAA -** Typically focused on the healthcare industry, but necessary for any company storing sensitive protected patient information.
- **PCI -** Compliance with the PCI DSS is required for any organization that stores, processes or transmits payment cardholder data.
- **ISO 27001 -** International Organization for Standardization (ISO) is an independent non-government organization and has international acceptance as a standards leader for electrical, electronic and related technologies.

Physical and virtual data center security and compliance practices are essential to successful organizations. With cyber warfare being launched by criminal organizations every day the necessity of state-of-the-art security has never been as critical. With attackers bypassing conventional security measures, many additional layers of cybersecurity and physical security measures are required to help mitigate your risk. Without these measures in place, your business could face some real challenges.

Cybersecurity Facts

Per a 2016 FireEyes report, **96%** of systems were breached on average. And 27 percent of those breaches involved advanced malware. All industries are a target but healthcare, retail and legal sectors saw major increases in breeches.

Over 169 million personal records were exposed in 2015, stemming from 781 publicized breaches across the financial, business, education, government and healthcare sectors.
– "ITRC Data Breach Reports – 2015 Year-End Totals" | ITRC

Ransomware Increased 35 Percent in 2015 - Cyber criminals are using encryption as a weapon to hold companies' and individuals' critical data hostage.
– "2016 CyberSecurity Threat Report" | Symantic

Symantec Blocked 100 Million Fake Technical Support Scams in 2015. Cyber scammers now make you call them to hand over your cash.
– "2016 CyberSecurity Threat Report" | Symantic

Ransomware is the most profitable attack to date, with as many as 90,000 victims targeted every 24 hours. Ransomware's victims are quite diverse and include most major industries, such as academic institutions, healthcare, law enforcement and even the federal government.
– Cisco's 2016 Midyear Cybersecurity Report

Cybersecurity spending to exceed $1 trillion from 2017 to 2021. The rising tide of cybercrime has pushed cybersecurity spending on products and services to more than $80 billion in 2016 *– Gartner*

The British insurance company Lloyd's estimates that cyberattacks cost businesses as much as $400 billion a year, which includes direct damage plus post-attack disruption to the normal course of business. Some vendor and media forecasts put the cybercrime figure as high as $500 billion and more
– http://www.csoonline.com/

OneNeck® IT SOLUTIONS
a TDS® Company

Part #3.1.2_AR_CYS_0117_v1

Call 855.ONENECK | Visit OneNeck.com