DATA CENTER SAFETY: 5 TRENDS TO INCREASE SECURITY

BY JOSH ABEBE | *Director of Industrial Sales*

The Data Center is an ever-evolving dynamic space. (According to Cisco, a data center is a physical facility that organizations use to house their critical applications and data.)

End users and owners need to be consistent in their strategies and implementation of corporate standards for the logical infrastructure (compute) layers and physical infrastructure layers that are most important for their security.

BEING INTENTIONAL WITH THESE STRATEGIES IS IMPORTANT

The benefits of logical and physical standards and architecture include lower installation cost, reductions in maintenance and move-add-change (MAC) costs, reduced downtime and a stronger infrastructure for securing data and facilities.

In 2020, 80.7% of organizations suffered from at least one successful cyberattack as noted in a 2021 Upsite Technologies article. More than a-third of organizations suffered six or more. The more data and information you store, the more appealing you become to outside threats. Security against internal threats is also a risk that must be mitigated, as more than 30% of those attacks come from internal breaches.

When creating standards, security should be paramount in any investment across the infrastructure. As a result, you can leverage these standards when improving or upgrading your infrastructure with products that are put on your networks to support, help maintain and improve your security outcomes.

WHY IS SECURITY SO IMPORTANT?

According to an SSL Store Hashedout blog, the data organizations obtain from employees, customers and consumers is exactly what cyber attackers are wanting. This information has a monetary value, not just to organizations who own it, but to those looking to steal it. Securing your information and data can have a positive impact resulting in customer loyalty, industry compliance and minimized financial exposure.

Let's look at trends that may impact on-premise (Enterprise or on Campus), cloud or colocation environments.

TOP FIVE SAFETY TRENDS FOR DATA CENTERS:

1 Increased Training: Companies like Cyberly and Techguard Security offer cybersecurity awareness training through online security training courses. These courses help corporations at all levels remain up to speed on the latest security threats and trends by giving people resources to mitigate risk through training and knowledge sharing.

2 Increased Security Spending: An Evoque blog about data center trends says, "the global data center security market is expected to triple in a seven year period from $6.9 billion in 2019 to $21.8 billion by 2026." This means more companies are committing to not just the use of data centers, but the means to protect them from threats as well.

3 Data Center Intelligence/AI & Automated Security Tools: The use of machine learning to aid in accelerating threat detection will complement the growth of automated security tools by giving IT workers the ability to focus on more complex tasks and strategy, according to a Data Center Dynamics blog.

Machine intelligence and automation streamline changes across multiple environments while providing agility and flexibility through change management. With the growth of remote workforce, data centers will require enhancements for securing workplace applications and sensitive data transmission like Multi-Factor Authentication (MFA) and other similar applications.

4 Change: As threats to data center security change, technologies built to protect must also evolve. The changing technologies have been constantly covering IoT devices as they increase in quantity and data capturing capabilities, edge computing (deployments will double by 2024), and a shift to cloud accelerating twice as fast as before the COVID-19 pandemic.

5 Shift Away from Traditional On-Premise to Hybrid Data Centers: Infrastructure strategies are now putting more emphasis on the people and their requirements for data versus the physical facilities themselves, according to a Gartner blog from 2019. Gartner predicted, by 2025, 80% of enterprises will shut down their traditional data centers.

A Paloalto blog notes an obvious trend is the move to a hybrid cloud, with many organizations looking to make their private data centers more "cloud" like. Infrastructure Strategies require agile network capabilities where an enterprise may or may not exist in the future. These networks need to be able to collaborate within the ecosystem and be scalable for remote growth. The majority of infrastructure strategies in the future will mix data center strategies in lieu of relying just on on-premise strategies. This will result in blending on-premise, co-location, cloud and edge compute strategies into a corporate data center strategy that supports the enterprise, remote and vendor ecosystems.

We can see how these trends are impacting global security spending. The data revolution continues and requires us to systematically process, upgrade and revisit our data center strategies.

If you would like to discuss your data center strategy, Kirby Risk can help. Reach out to your Account Manager or Network Consultant. You can also visit the *Connected* website.