Guidepost

SIX STAGES OF SECURITY DESIGN FOR DATA CENTERS

As more companies move their critical workloads and services to hosted servers and cloud computing infrastructure, data center security – the policies, procedures, and technologies that secure the center from cyberattacks and other threats – becomes more critical.

Security is fundamental to delivering a world-class enterprise system. For owners and operators of data centers, security must be the number one priority as they build, maintain, and scale operations for future growth. A single breach in the system can cause havoc and lead to reputational damage and loss of customer trust, noncompliance fines from regulators, and even financial damage resulting from downtime. Fabricating a secure data center security design and ensuring continuous and secure operations is essential.

Keeping data safe requires a best practices approach to security controls and a commitment to system checks that consider everything from site selection and the building itself to the software systems and personnel. Every component of a data center's security plan should be implemented with the other components in mind so that they form an interconnected network, each measure enhancing the effectiveness of the others. Physical security systems must be bolstered by a comprehensive set of processes and procedures so that data center personnel are working with clear guidelines when carrying out daily operations and dealing with irregularities.

In the video below, Michael Reyes discusses the Six Stages of Security Design for Data Centers. From design and installation to commissioning and the ongoing health of your security systems, we aim to keep you, your business and operations moving forward.