Cybersecurity: It's More than Just Technology

HOW THE ROLES OF COMPLIANCE AND PHYSICAL ACCESS ENSURE VIRTUAL SECURITY FOR THE ENTERPRISE

The term "cybersecurity" is commonly associated with the protection of digital data from theft or compromise by hackers. For enterprise customers, however, most data breaches aren't the result of technology villains inventing new ways to do damage.

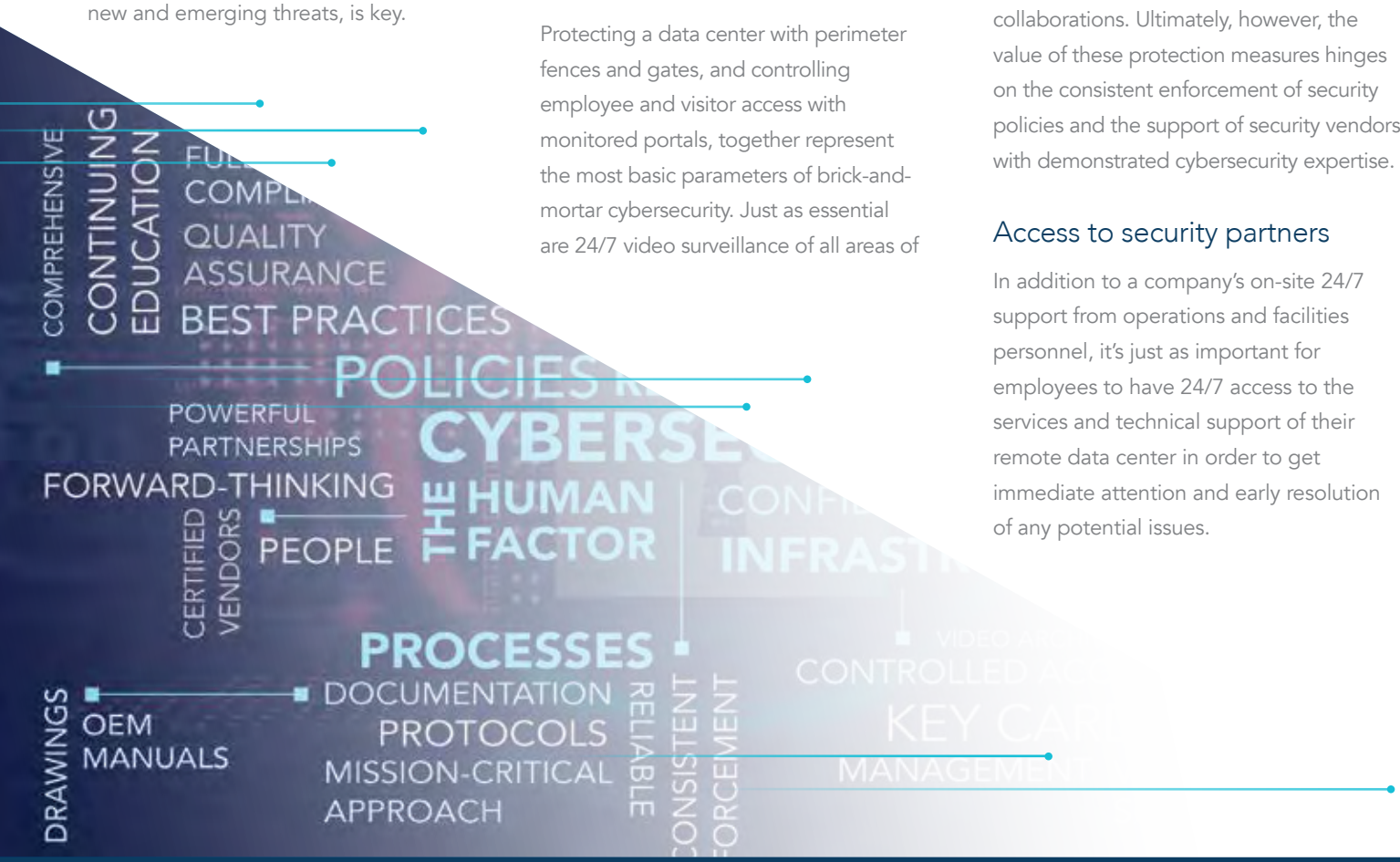
Instead, breaches are due to shortfalls in the development and enforcement of stringent security processes and protocols. This is why a good cybersecurity plan starts with a ground-up approach, including not only the technology and virtual security in place, but also very stringent physical security, backed by rigorously tested procedures and clearly defined business protocols.

The reality is that effective cybersecurity requires more than just a secure infrastructure and one-time installation of security processes. Cybersecurity requires ongoing attention to, and adjustment of, operational protocols and facilities management. The best strategy for ensuring it all: reliance on a data center with a strong and comprehensive mission-critical approach to business — including the support of experts whose sole focus is to collaborate with enterprise customers to enhance security and thwart cyberattacks.

Sound complicated? It's really not. By relying on a top-tier data center provider, businesses can focus on delivering on the promise to their own customers, confident that best-in-class compliance practices are being employed in the following key areas beyond the physical infrastructure itself.

Evergreen best practices

Times change. Cybersecurity threats are continually evolving. As a result, what's currently defined as a "best practice" could be outdated in a matter of months. Continually reviewing the details of internal operational procedures, in conjunction with staying up to speed on new and emerging threats, is key.



More often than not, staying ahead of the bad guys requires only minor adjustments to security measures already in place — but without an ongoing, top-to-bottom analysis of existing processes, even a minor security weakness or oversight could open the door to crippling damage.

24/7 monitored access

Protecting a data center with perimeter fences and gates, and controlling employee and visitor access with monitored portals, together represent the most basic parameters of brick-and-mortar cybersecurity. Just as essential are 24/7 video surveillance of all areas of the facility (with an appropriate archive of recorded footage); multi-factor access control (like key cards, locks or biometric authentication) of users for some areas or activities (or the ability to add such protection incrementally); required presentation of government-issued photo IDs for all visitors; and secure areas within the center for employee meetings and collaborations. Ultimately, however, the value of these protection measures hinges on the consistent enforcement of security policies and the support of security vendors with demonstrated cybersecurity expertise.

Access to security partners

In addition to a company's on-site 24/7 support from operations and facilities personnel, it's just as important for employees to have 24/7 access to the services and technical support of their remote data center in order to get immediate attention and early resolution of any potential issues.

Up-to-date operational certification

Earning operational certifications, such as Uptime (M&O), PMP, and ITIL, is highly important — not only to ensure optimal delivery of service, but also to enhance a data center's credibility to potential customers. It's also important to have certifications to ensure operational consistency across a portfolio of critical facilities.

Always-current documentation

Beyond expert hands-on operations, it's equally important to maintain thorough documentation and compliance procedures, such as drawings, OEM manuals, and operating policies. Technical and facility support should be 24/7, both on-site and remote, for immediate attention and early resolution of potential issues. Businesses can also benefit from the documentation and follow-through on a continuing-education policy for all personnel — not just engineers — to build and sustain a best-in-class operation.

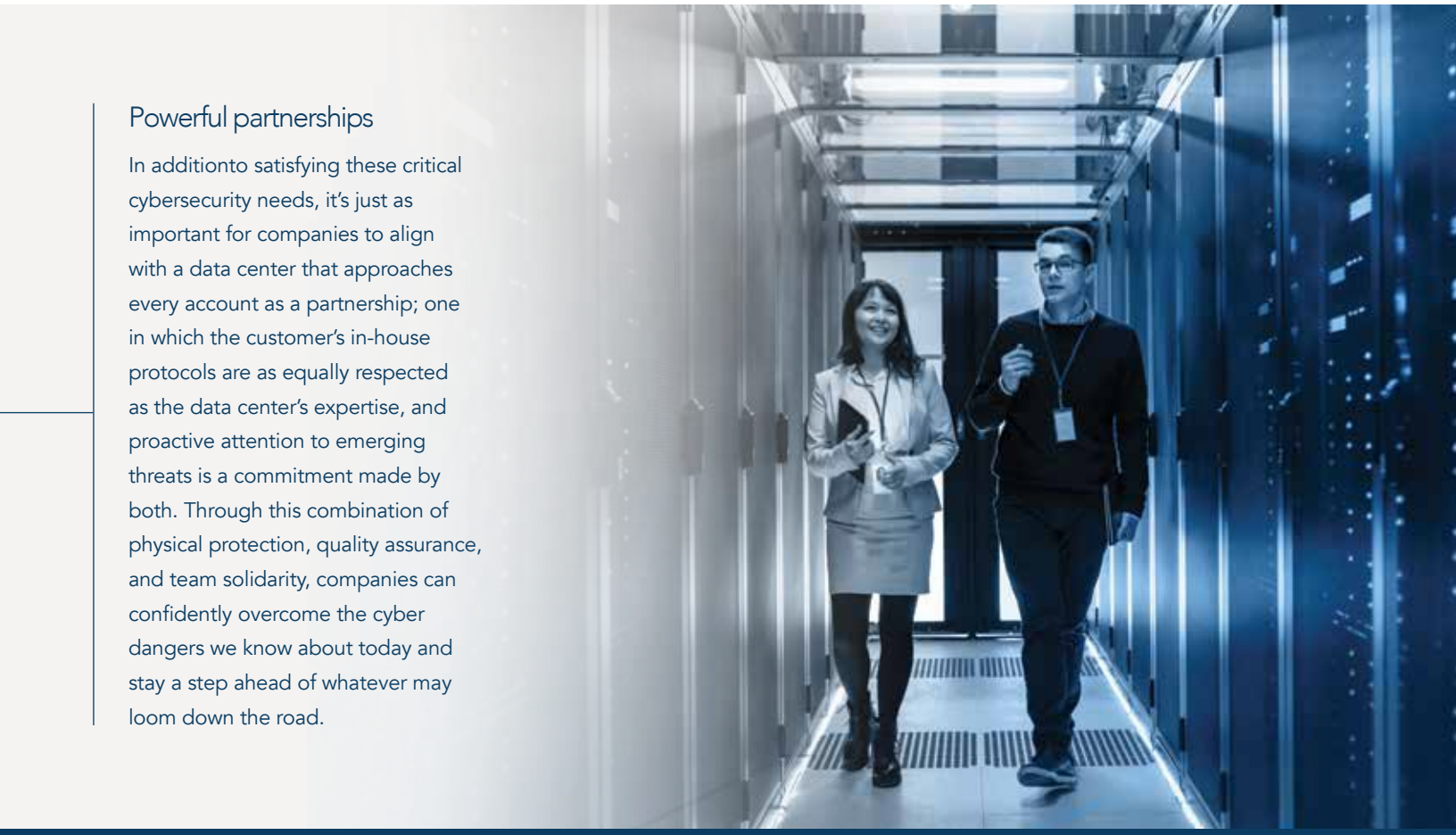
Full compliance

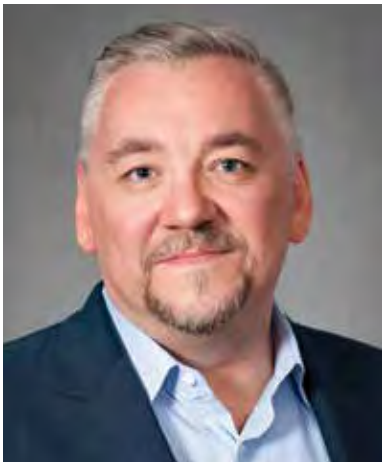
Controlling and securing data reliably, and responding successfully to rigorous audits, can be daunting. Meeting compliance mandates, however, will not only ensure maximum security and availability, but also enhance a data center's reputation for quality. Important compliance standards include, but are not limited to:

- NIST 800-53 PE and FISMA
- SSAE-18 (SOC 1) / ISAE 3402
- PCI DSS
- HIPAA
- HITRUST
- ISO27001

Powerful partnerships

In additionto satisfying these critical cybersecurity needs, it's just as important for companies to align with a data center that approaches every account as a partnership; one in which the customer's in-house protocols are as equally respected as the data center's expertise, and proactive attention to emerging threats is a commitment made by both. Through this combination of physical protection, quality assurance, and team solidarity, companies can confidently overcome the cyber dangers we know about today and stay a step ahead of whatever may loom down the road.





STEWART COLLIER

Managing Director, Critical Environments | Stream Data Centers

Stewart Collier leads the Critical Environments Services practice, or CES, at Stream Data Centers As Managing Director of Critical Environments, Collier runs a cross-functional team responsible for operating all data center facilities that Stream owns and manages.

Stewart also manages the Critical Environments Training Academy, or CETA, which provides Stream's data center team with industry-leading education in areas such as health and safety, cross-functional skillset development, and human factors training.

ABOUT STREAM DATA CENTERS

Stream Data Centers has been providing premium data center solutions and optimized value to Fortune 500 companies since 1999. To date, Stream has acquired and developed more than two million square feet of data center space nationally, representing more than 200 megawatts of power.

Stream is dedicated to improving the data center experience through exceptional people and service, developing and operating highly resilient, scalable and efficient data centers. Stream's product offerings include fully-commissioned Hyperscale Data Centers, Private Data Center™ Suites, Ready-to-Fit™ Powered Shells, Build-to-Suit Infrastructure and Retail Colocation Environments – all with immediate connection to network carriers and public cloud providers. See what's new at www.streamdatacenters.com.

Stream Data Centers is a subsidiary of Stream Realty Partners, L.P., a full service commercial real estate investment, development, and services company. Founded in 1996, Stream Realty has a staff of more than 750 real estate professionals with offices in 12 markets across the nation. The company manages 158 million square feet of commercial properties and completes approximately $3 billion in transactions annually. Learn more at www.streamrealty.com.