A JOURNAL
FOR BUSINESS
AND INDUSTRY

March + April 2020

Grayway

IoT Driving Demand for Data Center Growth

Data Security Breach Prevention and Protection

As Big Data Grows, Data Centers Add More Capacity and Security

Welcome.

Stephen Gray
PRESIDENT AND CHIEF EXECUTIVE OFFICER

As I write this letter, I realize we're all living in an unprecedented time. However, we've made a commitment to our customers and business partners to deliver on our promises, and one of these promises is to continue sharing industry trends with you.

Today, information is at our fingertips. We've all become accustomed to instant gratification. With this type of demand, it's no wonder that the global data center market is experiencing rapid growth with no expected slowdown.

In this issue of the GrayWay, we explore the growth drivers pushing the mission critical market forward. This topic cannot be discussed without talking about privacy and security measures, both of which are vital to consumers and network service providers. As you digest this information, we hope you have a clearer understanding of not only the market, but also where it's heading into the future.

FSC www.fsc.org
MIX
Paper from responsible sources
FSC® C016583

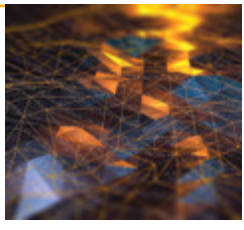
Gray practices methods which protect our environment.

Data Centers Add Value with New Business Models, Technology, and Security Measures

What's on the Inside. →

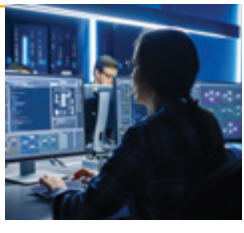
2 **The Data Center Industry Is Booming**

In this age of data, there are currently about seven billion Internet-connected devices, and that number continues to grow. Many of these generate large masses of data that must be captured, routed, stored, evaluated, and retrieved.



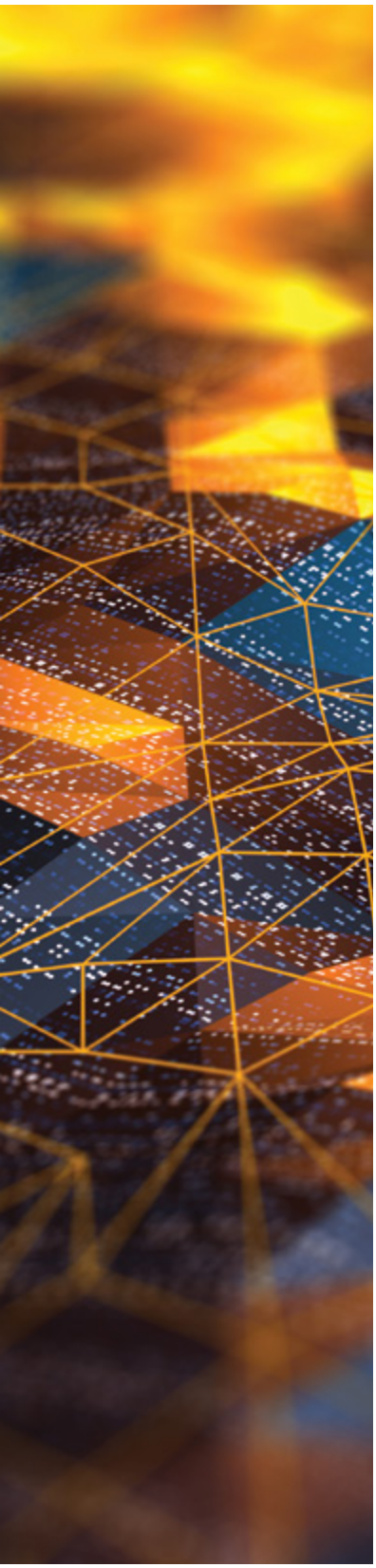
6 **Safe and Secure: Security Measures for Data Centers to Continue to Evolve**

As we generate and access more data, especially via websites, social networks, and electronic devices, there is greater opportunity for our personal or strategic data to be hacked.



9 **GRAY — We're Building**

With Gray's 60-year history in the industrial sector, we are more than equipped to meet the unique challenges data centers require.



The Data Center Industry Is Booming

Thanks to the Internet of Things, data centers are in high demand.

In this age of data, there are currently about seven billion Internet-connected devices, and that number continues to grow. Many of these generate large masses of data that must be captured, routed, stored, evaluated, and retrieved. With the rise of the Internet of Things (IoT) and Industry 4.0, manufacturers are relying on big data and data analytics to enhance the efficiency, productivity, security, and cost-effectiveness of their operations.

However, it is increasingly difficult, time-consuming, and expensive to manage data in-house. Even large companies like Cisco are considering shutting down some of their own internal data centers to save energy and infrastructure costs.

The solution? **Outsource data management.**

← *Back to Table of Contents*

More companies are outsourcing their data operations to third-party providers that specialize in data center operations. Colocation data centers are especially popular because they provide physical space, power, and cooling systems for servers and connections to local communication networks. Large colocation providers include QTS, Equinix, Digital Realty, Compass Data Centers, and Cologix, which provide rentable space up to 100,000 square feet or more.

Digital Realty's 365 Main data center in San Francisco, CA. Digital Realty Trust is the world's largest wholesale data center provider.

According to a recent report from Research and Markets, the global data center market is expected to grow at a compound annual growth rate of over 2% during the period 2019-2025. In the U.S. alone, the data center market is expected to reach revenues of over $69 billion by 2024. The greatest investments in data centers are from colocation service providers and hyperscale data centers (owned and operated by the company it supports, such as Apple or Google). In the U.S., the strongest growth is occurring in the Southeast and Pacific Northwest.

Key Drivers of Growth

The insatiable desire for data to improve business performance is driving the growth of the data center industry. Key factors include:

- Internet of Things—the U.S. is one of the leading markets for industrial IoT-driven technologies, including artificial intelligence, data and analytics, security, and communication
- Cloud storage—the use of cloud computing services and applications continues to grow rapidly in the U.S., thereby leading to the establishment of large colocation cloud-based data centers
- Submarine cable projects along the east coast—these bring extremely high-speed data from Europe and South America to the east coast, where it is routed to data centers where they come ashore (for example, Virginia Beach)
- Tax incentives—in recent years, data center growth has been concentrated in regions that provide tax incentives, including state and local governments that provide investment incentives (often energy-based)

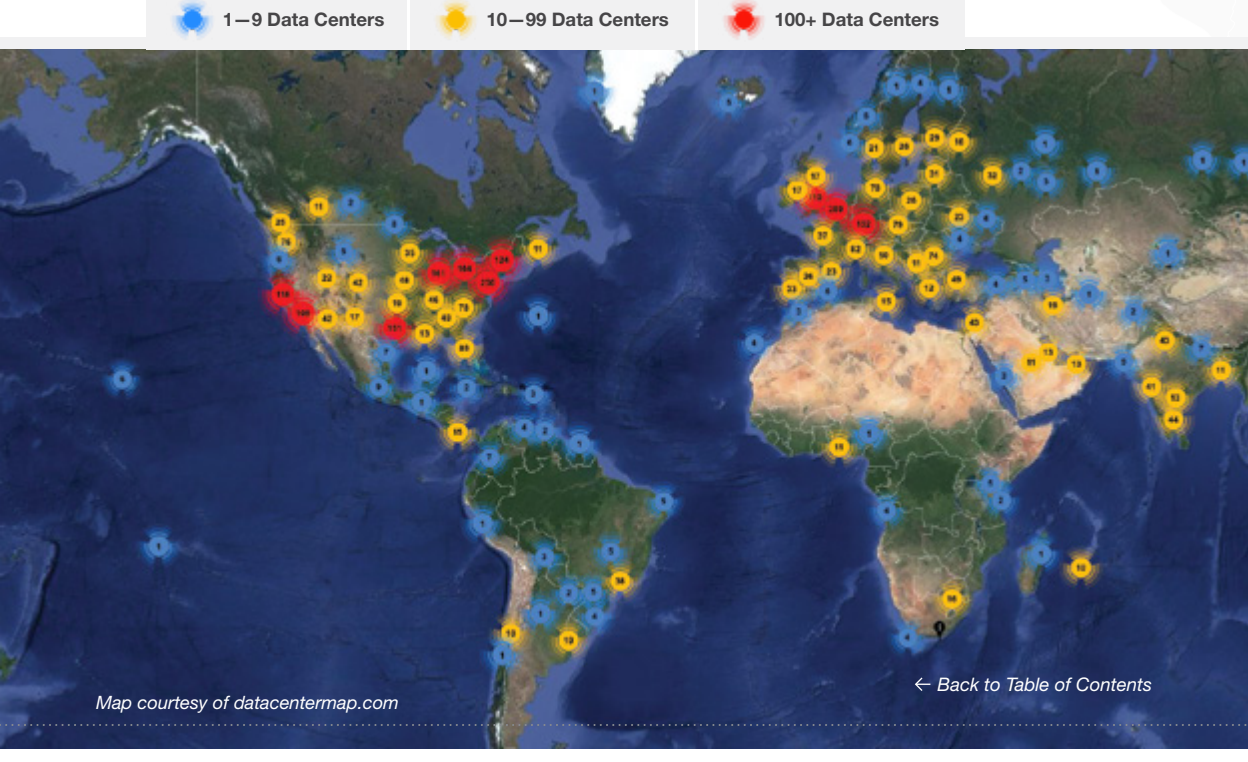
← Back to Table of Contents

Steady Investment

To meet these growing data needs, more data centers are being constructed—ranging from Tier 1 facilities (least complex and secure) to Tier 4 (very complex with high IT/security requirements), which are typically hyperscale centers. Favorable locations have low energy costs and top-notch communications infrastructure.

Colocation and managed services are in high demand—for example, over 300 colocation projects have been built in recent years, which include both new and expanded facilities. Major hyperscale projects are also being developed in China, Australia, Hong Kong, and India.

As companies move away from owning and operating their own data centers, they often leave behind abandoned space that can be upgraded into modern data centers. When these operations are well-located, with good supporting infrastructure and low energy costs, colocation service providers may purchase them. For example, California-based Equinix, one of the world's biggest data-center colocation providers, recently purchased 24 data-center sites from Verizon Communications for $3.6 billion.



Map courtesy of datacentermap.com

← Back to Table of Contents

Meeting Future Storage Needs

Data-center providers cannot build enough new capacity to meet demand. As new applications for technologies such as artificial intelligence and machine learning continue to grow, so do the needs for next-generation strategies and technologies to transform how we store, manage, and move data. For example, machine-to-machine technologies continue to generate enormous volumes of data, which are expensive to transmit. One solution being considered is integrated colocation and/or cloud partner ecosystems, where data centers are interconnected and collaboratively support each other and share assets, creating larger-scale data center districts or corridors.

Data-center efficiencies can also be improved through automation, where a single administrator can manage thousands of servers. This effort of automation is being led by advanced IT equipment and data center infrastructure management software providers. Some solutions even include robotics—for example, TMGcore has created a robot-managed immersion bath that can swap out a failed server and replace it with a fresh server.

"There is growing expectation that we are nearing an inflection point for change in how we manage data. We have begun to hit the wall in terms of machines working well in a human environment. It is now time for Version 2 of the data center, which will be an environment that is optimized for machines."

Scott Noteboom, CTO of Submer
IMMERSION COOLING PROVIDER

← *Back to Table of Contents*

Safe and Secure: Security Measures for Data Centers to Continue to Evolve

As we generate and access more data, especially via websites, social networks, and electronic devices, there is greater opportunity for our personal or strategic data to be hacked. With more data access points than ever before, the complexity, frequency, and expense of data breaches is ever-increasing.

3,800+

DATA BREACHES REPORTED IN 2019

$150M+

AVERAGE COST OF A DATA SECURITY BREACH FOR A MAJOR BUSINESS

In the U.S. alone, the number of data breaches per year has steadily grown from about 1,000 cases in 2014 to more than 3,800 data breaches reported in 2019. The average cost of a data security breach for a major business is over $150 million. Recent high-profile hacks include Facebook (2018, 50 million accounts) and Quora (2018, 100 million accounts). For businesses, ransomware is especially troublesome, with nearly 1,000 attacks in the U.S. in 2019.

Protecting Data Centers from Attack

A data center can be attacked by both internal and external sources. Nearly 35% of all data breaches are "inside jobs," carried out by dissatisfied employees. Physical security of the data center is therefore essential for ensuring that only authorized personnel have access to their specific areas. This is accomplished by:

- Zero trust model. Authentication and/or other credentials are required for all individuals with access to the data center and for all internal traffic.

← *Back to Table of Contents*

In 2019, Verizon's annual Data Breach Investigations Report found that more than one-third of all data breaches that occurred that year (nearly 35 percent) were the result of "insider threat actors."

- 24/7 security. On-site security starts with 24/7 security staff who patrol every data center zone. Other security assets include cameras, alarms, and security checkpoints.
- Background checks. Thorough background checks should be conducted for all operational staff, security staff, and third-party personnel who have access to the data center.
- Exit procedures. When someone with the authority to access sensitive zones and assets within the data center leaves their position, systems and procedures should be in place that specifically look for and remove these privileges.
- Biometric technology. Biometrics identify people through unique physical characteristics, such as fingerprints or the shape of a retina. It is especially valuable as a component of two-factor authentication.
- Secure access points. Entrances to sensitive zones like the data floor should be protected by multiple systems, including manned checkpoints, camera systems, and two-factor authentication.

Virtual Security Practices

Data protection starts with layered security measures. Each aspect of a security program should be integrated together as part of a comprehensive, layered system. Interconnected security protocols make it far more difficult for intruders to access valuable data or hardware assets in the data center. Other key data-protection recommendations by

← *Back to Table of Contents*

This simple diagram illustrates the three key components to creating an effective strategy for information security.

vXchnge, a data-center-as-a-service provider, include:

- Strengthen perimeter security, firewalls, and intrusion detection systems (IDSs) that monitor and inspect traffic before it reaches your internal network. They can detect any unusual activity of users or indicators of distributed denial-of-service (DDoS) attacks and other threats.
- Access control lists (ACLs). Most modern firewalls come already equipped with ACLs, which allow or deny traffic to specific areas.
- Two- and three-factor authentication.
- Penetration testing. Conducted annually, or even twice a year, penetration testing should be carried out by a verified third party, with any identified security risks fully mitigated.
- Radio-frequency identification (RFID) tagging allows staff to watch every piece of hardware 24/7/365. Tags can even send out alerts the moment an asset is moved or tampered with.
- Redundancy. Tier 3 or 4 data centers are typically larger and more complex systems that require more sophisticated and extensive security measures, including redundant infrastructure.
- Encryption. All data must be heavily encrypted during transfer and regularly backed up.

Moving Forward

Confidentiality, integrity, and availability (CIA Triad) are essential components of any effective information security program. The CIA triad is a widely used information security model that can guide an organization's efforts and policies aimed at keeping its data secure.

Every element of a data center's physical security should be implemented with other elements in mind so that they form an interlocking network of security measures, each one enhancing the effectiveness of the others.

Thorough security protocols should be regularly tested and upgraded as needed to keep pace with increasingly sophisticated cyber threats. As data center security technology continues to evolve, "new physical security measures will surely be incorporated as best practices," adds vXchnge. "Data center customers can review security certifications and request a more detailed overview of the physical and logical security measures a facility has put in place to ensure that data remains well-protected."

← *Back to Table of Contents*

Gray—We're Building

LEADING THE WAY IN THE MISSION CRITICAL MARKET

With Gray's 60-year history in the industrial sector, we are more than equipped to meet the unique challenges data centers require. Gray has built mission critical facilities for domestic and international customers, including a tier 4 facility, which house cloud-based services.

At Gray, we recognize the sensitivity and security necessary for these facilities. Going above and beyond all that is fundamental, Gray calculates what's needed for efficiency, speed to market, and reliability so our customers don't have to.

We build scalable end-to-end solutions with systemic redundancy and reliability in mind, delivering intelligent infrastructure that's pressure-tested to deliver continuous uptime. Serving all tier data centers, our team turns your challenges into opportunities.

From concept to commissioning and beyond, you can count on Gray to make your vision a reality.

Sample Projects

Confidential Customer
OREGON

210,000 s.f.

Greenfield data center on same site as a current Gray project underway.

Construction management and installation of owner provided equipment.

Confidential Customer
OREGON

215,335 s.f.

Greenfield data center and office on 78 acres.

Construction management and installation of owner provided equipment.

Confidential Customer
COLORADO

222,000 s.f.

Greenfield data center and office on 22 acres.

Construction management and installation of owner provided equipment.

← Back to Table of Contents

Gray®

Working with domestic and international customers to build a stronger future, **together.**

10 Quality Street
Lexington, KY 40507-1450

T: 859.281.5000
F: 859.252.5300

gray.com