#befutureready

INDUSTRY TRENDS

Government Goes Digital to Elevate the New, Open CX - Citizen Experience

THE INTERSECTION OF **INTERCONNECTION**

CORESITE
An American Tower Company

Introduction

Governments are making sizable investments in digital government initiatives. According to Gartner®, digital transformation, leveraging data effectively and technology modernization are the top three priorities of government CIOs. Worldwide government IT spending is forecast to total $588.9 billion in 2023, an increase of 6.8% from 2022, according to Gartner, Inc.[1] "Government organizations are continuing to modernize legacy IT and invest in initiatives that improve access to digital services as constituents increasingly demand experiences that are equivalent to online customer interactions in the private sector," said Daniel Snyder, Director Analyst at Gartner.[1]

While transformation is occurring across many fronts, including cloud adoption, data analytics, application development and collaboration with other agencies and third parties, the throughline is customer experience, or more specifically in this case, citizen experience (CX, for this white paper).

Agency goals focus on:

- **Building trust through transparency**
- **Adopting modern tools and technologies**
- **Streamlining service delivery**
- **Strengthening cybersecurity and hardening physical security**

Whether in the private or public sector, digital transformation strategies evolve, often in response to industry trends and infrastructure requirements. This paper explains why agencies are partnering with colocation data centers to achieve their IT modernization and CX goals. But first, let's set the stage by describing digital government.

What Is Digital Government?

The U.S. Department of State leads the charge for digital government development. In May 2012, it announced the Digital Government Strategy to deliver better digital services to citizens. The strategy involves sweeping changes – for example, implementing modern platforms that help eliminate IT silos, supporting digital identities, enabling data analytics and engaging partners.

Numerous objectives are mentioned in an Executive Order issued in December 2021. These include accountability, delivery of equitable services that everyone can navigate, efficiency, customer experience, human-centered design and other CX strategies. Additionally, the Order aims to maintain or enhance citizen protections put in place by law and policy. These include civil rights, privacy and information security.

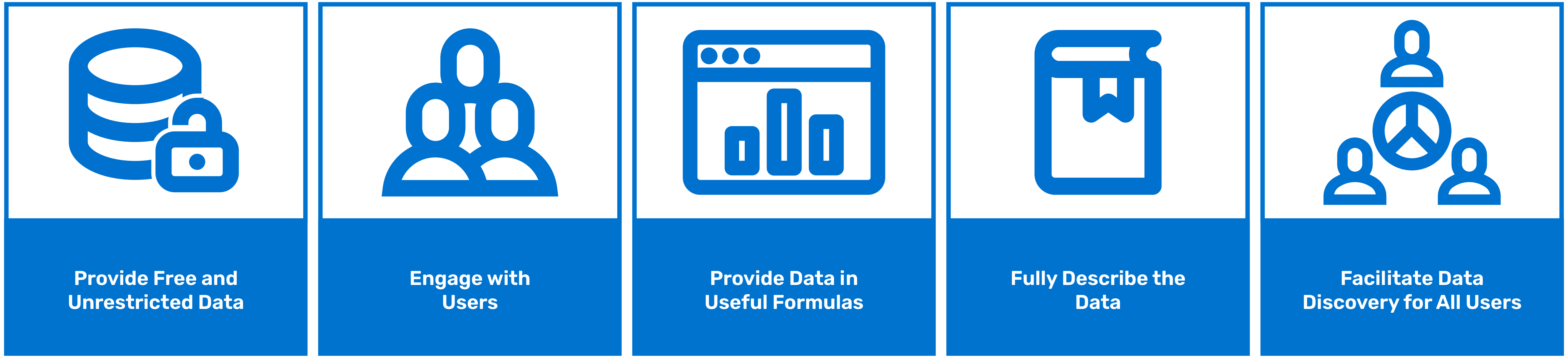
One strategy component - open data - aims to build trust and transparency. The Open Government Initiative is intended to "usher in a new era of open and accountable government" through records, reports and resources. Agencies are instructed to "open their doors and data to the American people."[2]

As digital government continues to unfold, decision-makers will have ample opportunities to address not only technology requirements but also issues such as responsible use of artificial intelligence (AI), the ethics that define digital interactions and citizen/data privacy practices.

Open Data

When data is open, it can be used and shared in a common, machine-readable format. Open data is meant to increase operational efficiency, to protect personal information and to enable public access to government information. Pillars of the Open Government Initiative are transparency, participation and collaboration.

5 Key Practices for Transparently Reporting Open Government Data



Provide Free and Unrestricted Data

Engage with Users

Provide Data in Useful Formulas

Fully Describe the Data

Facilitate Data Discovery for All Users

FIGURE 1: The process for reporting open government data is designed to increase transparency and build trust. Image courtesy U.S. Government Accountability Office.

Trends Highlight Customer Service Opportunities and Challenges

Trend insights help decision-makers set priorities, schedule and spending. Let's touch on three trends that can have a significant impact on CX.

1. Automation

According to Gartner, "75% of governments will have at least three enterprise-wide hyperautomation initiatives launched or underway in the next three years."[3] Hyperautomation, as defined by IBM, means "automating everything in an organization that can be automated."[4] Here are two examples.

Artificial Intelligence as a Service (AIaaS)

AIaaS-based services include chatbots, virtual assistants and speech-enabled applications. Behind the scenes, AIaaS allows agencies to quickly implement AI-based tools that can handle diverse customer data in various formats. Natural language processing tools use predictive capabilities to answer questions, summarize reports, classify documents and more.

Security, however, may be an issue. AIaaS suppliers access agency data, increasing third-party risk. Authentication methods and data protection must be rock-solid. Transparency might not be fully possible because subscribers of AIaaS do not see into the actual AI product. Nonetheless, AIaaS is an increasingly popular automation solution.

Do you know Emma, the chatbot that interacts with users of U.S. Citizenship and Immigration Services? Emma helps customers by answering questions about services, passports, green cards and more in both Spanish and English.

Mobile Government (mGovernment)

mGovernment services, which depend on mobile wireless technologies, greatly expand agencies' ability to reach people who don't have access to wired internet or prefer to use smartphones and the "anytime, anywhere" flexibility these devices offer. Familiar services include subscriber texts from a city's emergency management office, app-based parking payments and app-based FEMA disaster information.

What hampers growth of mGovernment services?
The lack of wireless/mobile infrastructure and limited service-areas prevent access, which are essential for citizen adoption. Also, security can be a concern because data travels over public wireless networks. However, the combination of an expanding wireless infrastructure, the boom in mobile apps and stronger cybersecurity measures point to higher future adoption.

2. Hybrid Cloud and Multicloud Adoption

Government agencies are revisiting how they use cloud, how it fits into their strategies and the cloud's role in digital services delivery – in large part because cloud benefits are so compelling. Decision-makers see the value in scalability, lower IT/operational costs and modern services and technologies.

A hybrid cloud deployment allows agencies to choose the best environment for data and workloads. Often, the most sensitive data stays in private clouds or on-premises data centers. Public cloud offers low-cost storage and easy access to less sensitive data. Multicloud enables agencies to use each cloud and cloud provider for a specific purpose – for example, customer authentication or platform as a service, which is a public network offering cloud access and application flexibility. Agencies can take advantage of each cloud provider's strengths, implement location-specific compliance and operate with more stability, because an outage in one cloud won't affect other clouds.

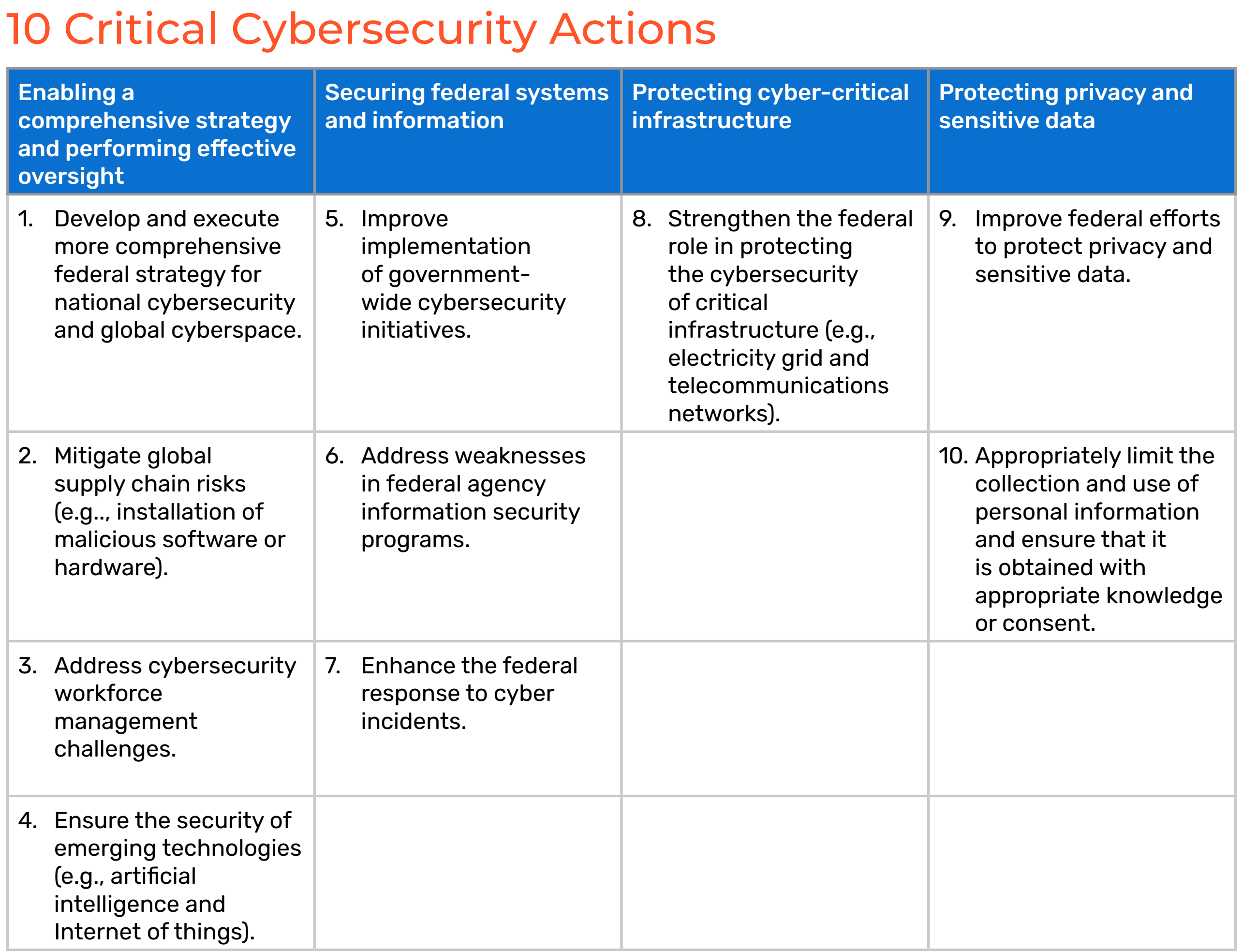
Centralized management is essential but not always seamless. Different providers have different shared responsibility models, service levels, application programming interfaces (APIs) and monitoring tools. As a result, cloud management can be complex and security inconsistent across clouds. Fortunately, there are management tools that offer cross-cloud visibility through a single view and simplified hybrid IT management.

3. Cybersecurity and Physical Security

In 2022, 25% of 550,000 federal employees polled in a survey worked remotely three or more days per week.[5] (The federal government employed 2.0 million people in 2020.[6]) Remote work has its advantages, but remote workers introduce vulnerabilities because connected devices, whose number keeps zooming upward, open new attack vectors. In response, the U.S. Congress recently funded cybersecurity initiatives for the Cybersecurity and Infrastructure Act (CISA), the Treasury Department and other agencies.[7]

How do funds help to enhance citizen and data protection? CISA priorities include removing barriers to threat information sharing between government and the private sector, enhancing detection of cybersecurity incidents on federal government networks and improving investigative and remediation capabilities related to intrusions. The Social Security Administration plans to accelerate multifactor authentication and strengthen system security. And, in 2022, the U.S. government outlined an investigative process to address security gaps related to 5G.

Yes, cybersecurity remains challenging, but improving it is a digital government centerpiece. The U.S. Government Accountability Office proposes 10 actions to help protect critical cyber infrastructure and data privacy.

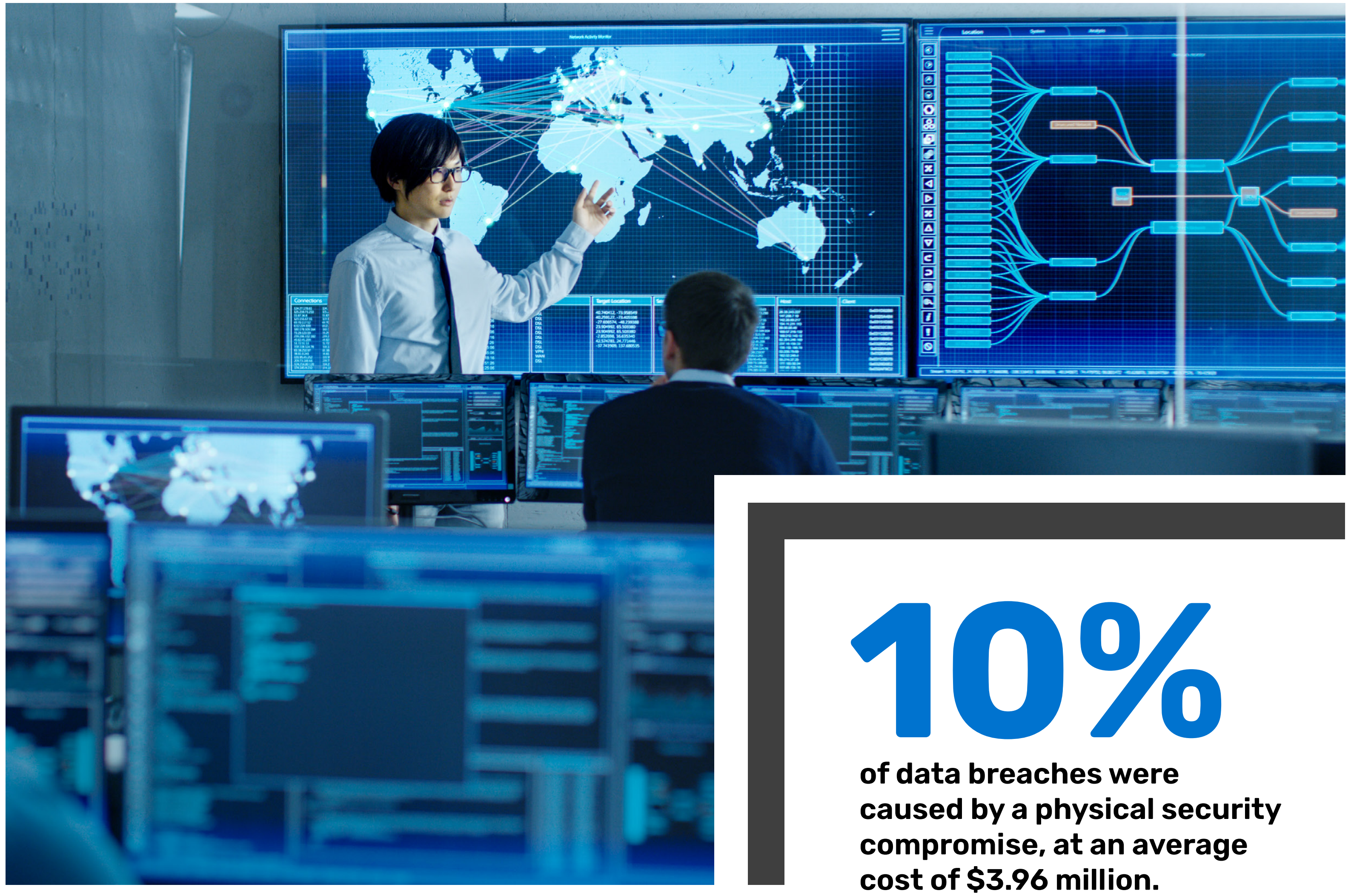


10 Critical Cybersecurity Actions

Enabling a comprehensive strategy and performing effective oversight	Securing federal systems and information	Protecting cyber-critical infrastructure	Protecting privacy and sensitive data
1. Develop and execute more comprehensive federal strategy for national cybersecurity and global cyberspace.	5. Improve implementation of government-wide cybersecurity initiatives.	8. Strengthen the federal role in protecting the cybersecurity of critical infrastructure (e.g., electricity grid and telecommunications networks).	9. Improve federal efforts to protect privacy and sensitive data.
2. Mitigate global supply chain risks (e.g.., installation of malicious software or hardware).	6. Address weaknesses in federal agency information security programs.		10. Appropriately limit the collection and use of personal information and ensure that it is obtained with appropriate knowledge or consent.
3. Address cybersecurity workforce management challenges.	7. Enhance the federal response to cyber incidents.		
4. Ensure the security of emerging technologies (e.g., artificial intelligence and Internet of things).			

FIGURE 2: The U.S. Government Accountability Office proposes 10 critical cybersecurity actions. Image courtesy U.S. Department of State.

Physical security complements cybersecurity in a comprehensive security posture. According to the 2022 Cost of a Data Breach Report, researched by the Ponemon Institute and published by IBM Security, about 10% of data breaches were caused by a physical security compromise, at an average cost of $3.96 million.[8] To be clear, the report is a global study of multiple industries, including public sector. The key takeaway is that physical breaches do occur, and on average take 217 days to identify and 63 days to contain.[8] It makes a strong argument for storing sensitive data in a data center, where trained security teams are on duty 24X7 and facilities include mantraps, biometric screening, video surveillance and other security hardening strategies beyond what on-premises data centers typically employ, even in government buildings.



10%

of data breaches were caused by a physical security compromise, at an average cost of $3.96 million.

Colocation Accelerates Digital Government and Public Sector Outcomes

Digital services increasingly rely on a hybrid IT infrastructure to keep up with technology innovations and deliver the desired outcomes – with CX at or near the top of the list. CoreSite provides customized hybrid IT orchestration solutions and modern, compliant data centers that offer a 100% uptime service level agreement (SLA) while helping you optimize cost, dynamically scale, manage risk and extend your IT team.

Colocation in a CoreSite data center enables:

- **Direct access to public cloud service providers that creates low latency, cost-effective broadband consumption and data transfer (most notability, data egress)**
- **Private, automated connectivity that bypasses the public internet and supports reliable, secure digital services**
- **Access to a large digital ecosystem of companies, including private cloud and as-a-service providers, with which you can partner to power your transformation strategy**
- **Interconnection capabilities, a competitive advantage that allows you to reach new geographic markets easily**
- **Multiple layers of physical security and trained and certified security personnel on site 24X7X365**
- **Single-pane-of-glass multicloud and hybrid IT management, enabled by a virtualized network services platform**

Let's elaborate on the last bullet. The Open Cloud Exchange® is a software-defined networking platform that provides automated, enterprise-class network services within CoreSite data centers. With it, you can quickly establish and deftly manage interconnection to public and private clouds, partners and all CoreSite data centers.

#befutureready

Learn How We Can Advance Your Digital Government Mission

While digital transformation objectives vary within federal, state and local governments, the one clear mission remains the same – to deliver open, accessible customer experience to all citizens.

When you're ready, talk to us about your goals, plans and risk tolerance. We can help you develop an IT modernization strategy that immediately delivers measurable cost and productivity benefits and ensures your agency is future-ready.

SPEAK WITH AN EXPERT

1. Gartner Press Release, "Gartner Forecasts Worldwide Government IT Spending to Grow 6.8% in 2023," December 12, 2022. https://www.gartner.com/en/newsroom/press-releases/2022-12-12-govt-it-spending-forecast-2023#:~:text=Worldwide%20government
2. Open Government Initiative, U.S. Department of State, 2023
3. Gartner Press Release, "Gartner Unveils the Top 10 Government Technology Trends for 2022," February 21, 2022. https://www.gartner.com/en/newsroom/press-releases/2022-02-21-govt-tech-trends-2022-press-release
4. What is hyperautomation?, IBM, 2023
5. Federal Employee Viewpoint Survey Results, U.S. Office of Personnel Management, 2022
6. Public service and the federal government, Voter Vitals, Bookings, 2020
7. CSO, U.S. Congress Funds Cybersecurity Initiatives in FY2023 Spending Bill, December 30, 2022
8. Cost of a Data Breach Report 2022, IBM and Ponemon Institute, 2022

Join the Conversation

@CoreSite

www.linkedin.com/company/coresite/

#befutureready

About CoreSite, An American Tower Company

CoreSite, an American Tower Corporation subsidiary, provides hybrid IT solutions that empower enterprises, cloud, network, and IT service providers to monetize and future-proof their digital business. Our highly interconnected data center campuses offer a native digital supply chain featuring direct cloud onramps to enable our customers to build customized hybrid IT infrastructure and accelerate digital transformation. For more than 20 years, CoreSite's team of technical experts have partnered with customers to optimize operations, elevate customer experience, dynamically scale, and leverage data to gain competitive edge.