Enabling confident decisions in data center environments

Beyond uptime: The risk you don't see

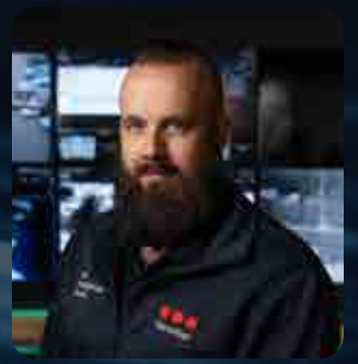


Securitas

Securitas Risk Intelligence

Contents

Methodology	4
Our intelligence toolkit	6
Key focus area 1: Activism & extremism	8
Key focus area 2: Nation State threats & information disorder	16
Key focus area 3: Localized backlash & political pressure	22
Key focus area 4: Colocation and CNI dependencies	28
Key focus area 5: Supply chain volatility	34



Ben Giddings
Protective Intelligence Manager

Introduction

Data centers have become a critical part of modern infrastructure, underpinning the services that businesses, governments, and individuals depend on every day, from cloud computing, AI, financial services, communications, healthcare, and national security.

As demand for digital services grows, so does reliance on the infrastructure that stores, processes, and transmits huge quantities of data. The rapid expansion of AI, global connectivity and digitization across sectors have elevated data centers from supporting infrastructure to business-critical assets. For many organizations, data center capacity has become a strategic requirement, with resilience essential to business continuity.

At the same time, the threat landscape is becoming increasingly complex. While traditional security concerns remain relevant, organizations must also contend with geopolitical tensions, activism, insider threats, cyber attacks, supply chain vulnerabilities, regulatory change, and environmental pressures, all of which can significantly affect operations, reputation, and growth.

These risks rarely occur in isolation. Events thousands of miles away can disrupt energy markets, critical mineral supply chains, technology dependencies, or regulatory environments. Equally, local incidents such as power outages or activist activity can escalate through media reporting and social media amplification.

In this report, we examine the most significant risks currently affecting the global data center sector. Drawing upon intelligence collected and assessed by our Risk Intelligence analysts, this report explores the key themes shaping today's operating environment and highlights emerging trends organizations should monitor in the years ahead.

The organizations best positioned to succeed will not necessarily be those that face the fewest threats, but those that identify, understand, and mitigate them. Effective risk intelligence provides decision-makers with the situational awareness needed to anticipate change, prioritize resources, and make informed decisions. As data centers continue to underpin the global economy and digital transformation, those that recognize emerging risks early will be better equipped to protect critical infrastructure, maintain operational continuity, and support future growth.

Team Members



Jessica Wilson
Risk Intelligence Analyst



Daniel Guzman
Protective Intelligence Analyst



Freddie Venables
Protective Intelligence Analyst

"Resilience is no longer defined only by an organization's ability to respond to disruption. It is increasingly determined by its ability to anticipate it."

Matt Ellis, President Security Risk Management, Securitas Group

This report has been developed by Securitas' Risk Intelligence Center (RIC), our dedicated unit for global risk analysis and strategic insight. The RIC continuously monitors geopolitical developments, emerging threats, and industry-specific risk patterns, transforming complex information into clear, evidence-based intelligence. Its work provides the analytical foundation for Securitas Risk Intelligence assessments and services.

Methodology

Threat levels

This report uses the RIC's threat level system to score threats on a 1-5 scale based on the assessed likelihood and severity, and / or intent and capability.

5 - EXTREME

Very high / extreme threat.
Review and respond if required.

4 - HIGH

High / major threat.
Consider taking appropriate action.

3 - MODERATE

Moderate threat.
Maintain awareness, cons. precautions.

2 - LOW

Low / limited threat.
Be advised.

1 - VERY LOW

Very low / insignificant threat.
For awareness.

Language of probability

The report uses the RIC's language of probability to provide an assessment of likelihood of a threat manifesting, based on probability, using a percentage, fraction, or ratio as a baseline. This helps to provide context and clarity and helps maintain a standardized approach.

Term	Probability
Remote	0-4%
Highly unlikely	10-20%
Unlikely	25-35%
Realistic possibility	40-50%
Likely/Probable	55-75%
Highly likely	80-90%
Almost certain	95-99%



Intent and capability

Level	Intent	Capability
5 - EXTREME	The threat actor / source is determined in its COA (Course of Action); there is a significant perception of mission success / reward; there is an established history / precedent of success.	The threat actor / source has all of the resources necessary to carry out its COA, and any constraints are highly unlikely to prevent it from carrying out the COA.
4 - HIGH	The threat actor / source has expressed its intent; there is perception of specific success / reward; there is a history / precedent of targeting.	The threat actor / source has access to the resources required for its COA, and while there are constraints these are unlikely to deter or deny it,
3 - MODERATE	The threat actor / source has an implied intent; there is perception of some success / reward; there is limited history / precedent.	The threat actor /source has some access to resources required for its COA, and there are some constraints which may deter or deny it.
2 - LOW	The threat actor / source has not implied intent though the target is perceived as viable to the COA; there is a low success rate / rate; there is no history / precedent.	The threat actor / source has limited access to the resources required for its COA, and there are numerous constraints which will likely deter or deny it.
1 - VERY LOW	The threat actor / source has not expressed or implied intent; there is very low / no reward and success uncertain; there is no history / precedent.	The threat actor / source has very limited access to the resources required for its COA, and there are significant constraints which will highly likely prevent it from carrying out the COA.

Our intelligence toolkit

Protect what matters with intelligence that drives action. Securitas Risk Intelligence delivers more than situational awareness, providing the context, foresight, and expert guidance organizations need to navigate an increasingly complex risk landscape.
Through a combination of digital intelligence tools, managed services, embedded analysts, and specialist consulting, we create tailored intelligence solutions that help organizations anticipate emerging threats, enhance resilience, and make confident, risk-informed decisions.

Embedded Analyst

Dedicated expertise.
Global reach. Local impact.

Embedded intelligence services place dedicated intelligence expertise directly within your organization. Fully integrated and supported by Securitas' global intelligence community, embedded analysts deliver tailored insights, proactive monitoring, and strategic decision support to help organizations anticipate risk, protect critical assets, and respond with confidence.

Includes:

- Dedicated analyst support integrated with your security and risk management functions
- Tailored intelligence production, threat monitoring, and risk assessments
- 24/7 reach-back support from Securitas' global intelligence community
- Access to training, thought leadership, intelligence briefings, and peer collaboration networks

Advisory

Specific & tailored intelligence

An all-in-one Protective, Threat and Risk Intelligence solution tailored to your organization, operations and brand.

Based on your specific intelligence requirements, Advisory provides ongoing monitoring and finished intelligence to help you understand what matters, why it matters and what to do about it.

Includes:

- Daily intelligence summary as per current service
- Immediate briefs for warning intelligence
- Threat, protective and risk intelligence
- Access to on-demand reporting services

Awareness

Global situational awareness

Stay ahead with regular scheduled and ad hoc reporting on the global security and threat landscape, helping you stay informed of significant developments and make informed decisions.

Includes:

- Daily global Intelligence reports
- Weekly global intelligence outlooks
- Monthly threat forecasts
- Monthly intelligence summaries
- Situation reports and Intelligence reports for significant developments

Alerting

Targeted location-based intelligence

Receive geo-targeted alerts for security and threat events near your locations. Alerts are fully customizable based on severity, proximity and frequency, helping you stay informed with notifications and early warnings for emerging threats.

Covers:

- Criminality
- Civil unrest
- Terrorism
- Weather
- Travel & transportation

Ad-hoc Intelligence

Intelligence when you need it

Subject matter expertise and consultancy for dynamic, specific intelligence requirements, from immediate updates and one-off reports to specialized intelligence requirements.

Common requirements include:

- Travel security
- Executive protection
- Defensive screening
- Event security assessments
- And more

Key focus area 1

Activism & extremism

Bottom line up front (BLUF)

Data centers are almost certain to face a sustained threat from activism, driven primarily by environmental concerns, anti-Artificial Intelligence (AI) sentiment, and sector / organization-specific controversies, which will highly likely become progressively entangled with extremist narratives, increasing the risk of hostile rhetoric, targeted intimidation, and sporadic violence directed at physical data center sites and C-suite executives.

Assessment

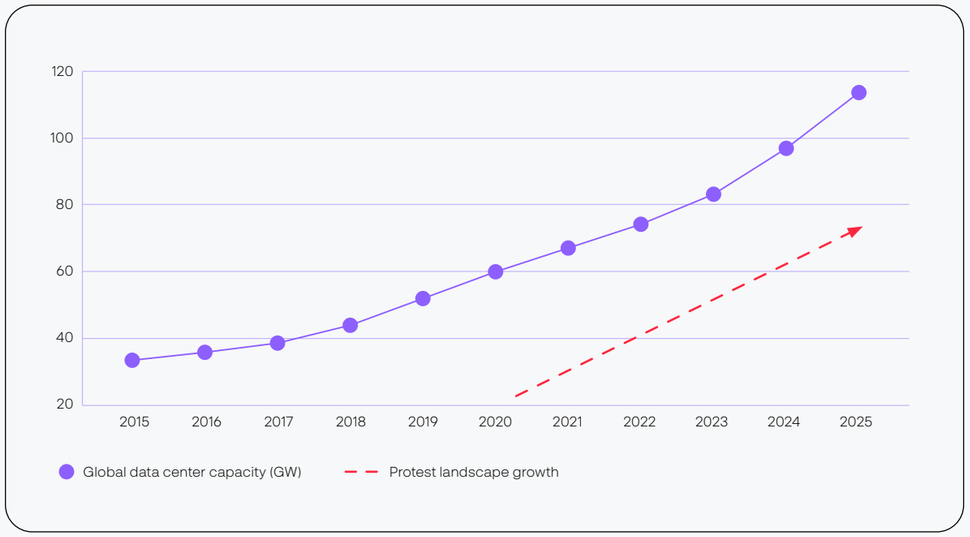
Threat level 4

Most likely course of action (MLCOA) vs Most dangerous course of action (MDCOA)

MLCOA: Data centers will continue to inspire activism concerned with the environmental and local impacts of the infrastructure, exacerbated by the sector's role in the development and expansion of AI, another highly contentious topic. While activists will show varying intent, motivation, and capability, sporadic escalations in tactics will complicate security postures and aim to hinder operations and damage assets, although efforts remain predominantly peaceful. The continued growth of the sector will push such narratives into the realms of extremist ideologies, promoting more violent / disruptive behavior that will threaten people, property, and operations.

MDCOA: Data center infrastructure becomes a primary target of activists seeking to slow the sector's growth through escalatory tactics, such as criminal damage, violence, and vandalism, which consistently degrade operations and incur significant financial repercussions. This will be consistent and repeated, with activists covertly organizing actions supplemented by information disorder campaigns online. Anti-technology extremism shows a rapid increase, correlating with the predicted growth of the data center industry, heightening the threat landscape posed against data centers and the operating organizations. This translates into direct risks against C-suite executives, deemed to personally reflect the morals and values of the organization and support all contentious business practices.





Graph to demonstrate the correlation between the growth of data centers and the expansion of the protest landscape against data centers. Source: data from GEP, table made by RIC.

Detail

Data centers have a significant environmental impact driven by high electricity consumption, water usage, and rising carbon emissions, concerns of which have only intensified since the rapid expansion of AI and the demand this creates for data centers, which far surpasses that of traditional cloud storage facilities. The growth of data center infrastructure and the expansion of the protest threat landscape are mutually inclusive; they serve as a highly visible symbol of environmental strain and corporate influence, which has incited a broad coalition of ideological actors whose narratives are amplified by information disorder and extremist rhetoric. This has moved opposition from local disputes and fringe communities to national coordinated movements, and in extreme circumstances, escalating hostility towards executives and physical assets.

North America

Graphics show the geographic spread of activism and direct action impacting the technology and data center industry across North America between July 2025-2026. (Source: RIC – MySecuritas App – Briefs & Events)



Europe

Graphics show the geographic spread of activism and direct action impacting the technology and data center industry across Europe between July 2025-2026. (Source: RIC – MySecuritas App – Briefs & Events)



Course of action analysis

Peaceful protests	Detail	While the intent, motivation, and capability of activist groups differ, this can involve small or large mobilizations, either remaining localized or organized on a national level to inspire country-wide actions. This often includes the use of posters, banners, chants, and noise protests.
	Threat level	2 - LOW
	COA probability	HIGHLY LIKELY 80-90%
Blockades	Detail	Blockades often impact entrance / exit to sites, impacting employee / goods mobility, and may also involve more disruptive TTPs such as sit-in protests to prolong disruption to the affected asset.
	Threat level	3 - MODERATE
	COA probability	HIGHLY LIKELY 80-90%
Escalation	Detail	Escalation by activists could include violence against a person, including employees and executives, or the targeting of property, such as criminal damage or vandalism.
	Threat level	4 - HIGH
	COA probability	REALISTIC POSSIBILITY 40-50%
Online campaigns	Detail	Activists often use online campaigns prior to physical actions to garner support and encourage people to attend the action. This is often in the form of imagery, an 'exposé' using open source information to 'reveal' controversial business practices / relations, and formulate accusations against an organization. This commonly features exaggerated claims, information disorder, and inflammatory language.
	Threat level	3 - MODERATE
	COA probability	ALMOST CERTAIN 95-99%
Extremism	Detail	There is an increasing convergence between activist and extremist ideology, complicating the threat landscape for many organizations and entities with the threat of targeting violence, including offenses against the person or offenses against property.
	Threat level	5 - EXTREME
	COA probability	LIKELY/PROBABLE 55-75%

Activism & extremism

Data centers offer tangible, highly visible physical assets that form a focal point of campaigns, making them susceptible to various tactics, techniques, and procedures (TTPs) ranging from influence campaigns, such as protests, picketing, and leafletting, to more disruptive TTPs aiming to disrupt operations, such as criminal damage and vandalism. Online campaigns often serve as pre-action indicators, aiming to raise awareness, garner support, and damage reputations, and wider organization-specific controversies, such as contentious commercial relations, can incite activism, notably with the increasing hybridization of campaigns.

Case study Netherlands

Environmental activists with Extinction Rebellion (XR) Netherlands and Geef Tegengas threw water balloons filled with a mixture of acetic acid, acrylic paint, hydrogen peroxide, and salt, intending to corrode the steel used at a Microsoft data center construction site near Sloterdijk Station, Amsterdam, Netherlands in July 2026. This action was motivated by the site's potential environmental impact, directly referencing electricity and water use, noise pollution, and greenhouse gas emissions, and denounced the organization's data center in Middenmeer, Netherlands, which allegedly stores phone calls made by Palestinians living in the Gaza Strip to coordinate airstrikes and arrests. The extent of the damage caused by this action has not been confirmed on open-source platforms.

Case study San Francisco

While the following case study does not specifically impact data centers, it demonstrates high-severity threats from anti-tech / anti-AI extremism, which will highly likely require consideration as AI and data centers become further interconnected.

A 20-year-old suspect was arrested on suspicion of throwing a Molotov cocktail at OpenAI CEO Sam Altman's home and making threats toward the AI company's headquarters in San Francisco, US, in April 2026, and was later found to possess a "three-part series" manifesto listing the names and addresses of other AI industry CEOs and executives. The suspect was allegedly motivated by anti-AI sentiment and was a member of the anti-AI activist group PauseAI. Two days later, two individuals were arrested for the negligent discharge of a firearm after allegedly firing a gun towards the San Francisco, US, home of Sam Altman; however, the motivation for this action is yet to be determined.



Advisory

- Maintain awareness of local and regional activist threat actors, including their organization, typical TTPs, and online footprint, and tailor on-site security measures to effectively and efficiently mitigate and defend against such threats.
- Establish incident response plans (IRPs) that respond to all possible activist targeting, making direct reference to vulnerable assets, employee evacuation, and contingency processes to allow for operational resiliency.
- Liaise with local authorities to facilitate intelligence sharing and determine when police intervention may be required.

Key focus area 2

Nation State threats & information disorder

Bottom line up front (BLUF)

Data centers are becoming an increasingly recognized strategic asset, exposing them to direct targeting from nation states through both kinetic warfare, physically damaging expensive infrastructure and hindering operational capacity, and information disorder campaigns, as a form of gray zone warfare (GZW) seeking to deepen existing domestic fractures.

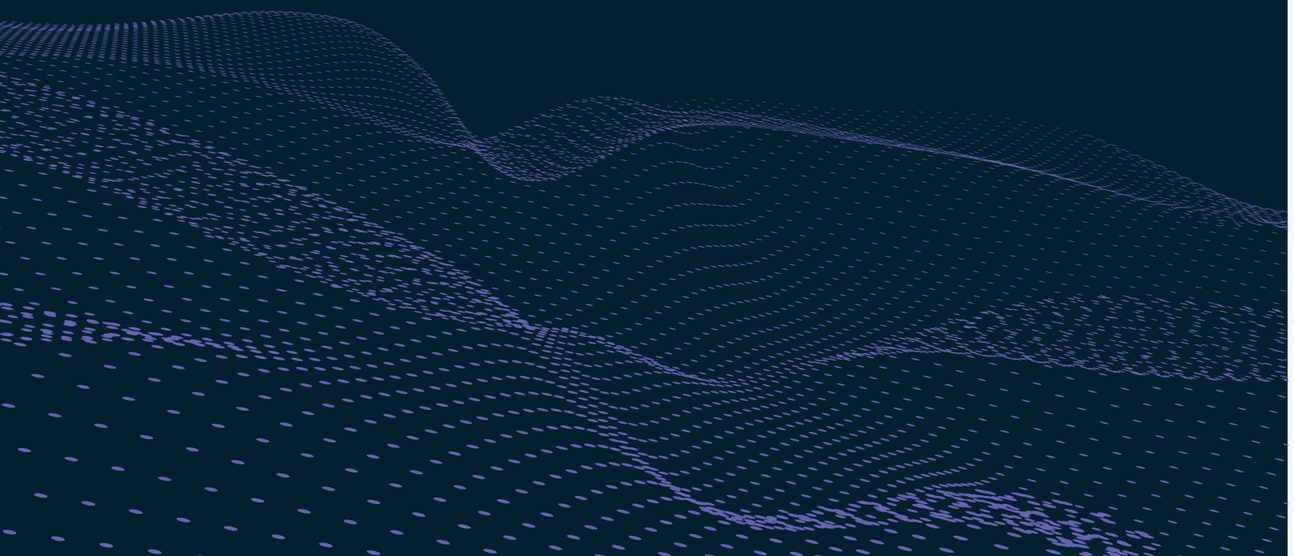
Assessment

Threat level 4

Most likely course of action (MLCOA) vs Most dangerous course of action (MDCOA)

MLCOA: Data centers are likely to become an increasingly important asset for countries / regions, enhancing commercial markets, telecommunication connectivity, and defensive capabilities. This will likely increase their attractiveness as legitimate targets for both military offensives and online information disorder campaigns, with nation-state threat actors likely recognizing that damage to such infrastructure can impact countries in various ways. This will likely become a quickly emerging security concern for all data center operators, likely prompting renewed standards and requirements for security postures around data centers.

MDCOA: Data centers become a normalized target during active offensives in the immediate term, allowing threat actors to disrupt civilian, commercial, and military operations before the requisite security measures can be implemented. This is supplemented by a significant increase in anti-data center sentiment from offshore networks, further fragmenting existing domestic polarization, impacting the response of the public and local authorities following the direct targeting of data centers during conflict.



Detail

Data centers are an emerging direct strategic target in modern conflicts, serving as physical infrastructure with symbolic value to undermine geopolitical and technological influence / alliance. Inherent to commercial facilities, data centers lack the military-style defense mechanisms required during active conflict and are therefore a vulnerable asset of high visibility and large scale. Their dual-use nature, hosting civilian commerce, military communications, AI modeling, and military intelligence, makes data centers an attractive target to cause widespread disruption beyond physical damage, such as financial markets, government operations, and defensive capabilities.

This was most recently demonstrated in the ongoing Iran conflict, in which Iran declared major US tech companies and regional data centers across the Middle East as legitimate military targets, specifically citing 18 target organizations including Amazon, Microsoft, and Google. This formed part of a pressure campaign against Gulf states hosting digital and physical alignment with the US.



Case study Iran

Iranian drone strikes repeatedly damaged an Amazon Web Services (AWS) facility in Bahrain between March and July 2026, forcing widespread application outages and emergency data migration as well as physical damage to its infrastructure. Various sectors were impacted, including higher education, finance, and telecommunications.

Data centers form a significant proportion of domestic socio-political tension, which has been recognized by international threat actors, such as China, Iran, and Russia, who repeatedly run online information disorder campaigns to exploit existing social divisions. This GZW tactic utilizes non-military methods to achieve geopolitical goals while staying below the threshold of traditional armed conflict, aiming to stall US technological progress, undermine trust in democratic institutions, and force critical infrastructure into a major political fracture point of anti-data center and anti-AI polarization. Information disorder campaigns are predominantly made up of AI-generated images echoing anti-data center narratives from state-linked social media accounts and news platforms, and articles written to deepen this divide.

Nation State threats & information disorder

AI generated image using Microsoft Copilot using the prompt ‘Please generate an image that portrays a data center looming over a village with residents looking worried about the water and energy usage in a cartoon format.’

An article was released by China Daily, a newspaper owned by the Publicity Department of the Chinese Communist Party, in March 2026, reiterating existing concerns held across the US about the impact of data centers on residents’ electricity bills.



AI-generated images have been posted to local social media pages, such as ‘Life in Oklahoma’ and ‘Only in Montana’, to reaffirm community concerns about data centers. These have been linked back to offshore networks.

An article was released by the Russian newspaper Pravda in May 2026, framing US technology organizations and data centers as *“unfavorable for ordinary people,”* and reinforcing anti-establishment rhetoric.



Advisory

- It is advised that the geopolitical exposure of data centers via geopolitical relations is consistently reassessed, considering indicators such as intensifying market competition, escalating military offensives, and strategic goals.
- While international propaganda is unlikely to have a significant impact on the broader anti-data center sentiment, it is advised that online propaganda is monitored and geographically mapped to identify possible patterns and trends.
- Organizations are advised to liaise with local and national security authorities, both public and private, to facilitate a uniform security posture across the data center sector that specifically addresses the volatility of targeting during active conflict.

Key focus area 3

Localized backlash & political pressure

Bottom line up front (BLUF)

Public opposition to data centers will almost certainly continue to mount, characterized by concerns over utility strain, environmental disruptions, and a lack of tangible benefits for local residents, commonly referencing water usage, noise pollution, increasing energy bills, and industrialization. This has served to actively shape local, regional, and state-level laws through zoning changes, construction moratoriums, and resource oversight bills, though federal policy remains largely pro-expansion.

Assessment

Threat level 4

Most likely course of action (MLCOA) vs Most dangerous course of action (MDCOA)

MLCOA: Data center demand will likely continue to gradually increase, inciting a growing threat landscape posed by localized backlash that will likely remain predominantly focused during the consultation period. This will likely prompt further patchwork legal and regulatory frameworks, continuing to complicate organizations' ability to balance operational and strategic needs with inconsistent planning and zoning requirements. Overarching governance from federal and national governments will likely remain pro-expansion, causing further contradictory narratives, and show a pattern alongside geopolitical and economic competition.

MDCOA: A rigorous pro-expansion direction is taken, overriding local laws that restrict permissions and disregarding possible dangers of a sudden increase in data center infrastructure for both local residents and the CNI it depends on. This creates a deeper divide between federal and local viewpoints, encouraging residents to take more direct action, possibly pushing them to activist groups that see an increased intent, capability, and motivation.



^ Source: Google Maps and RIC

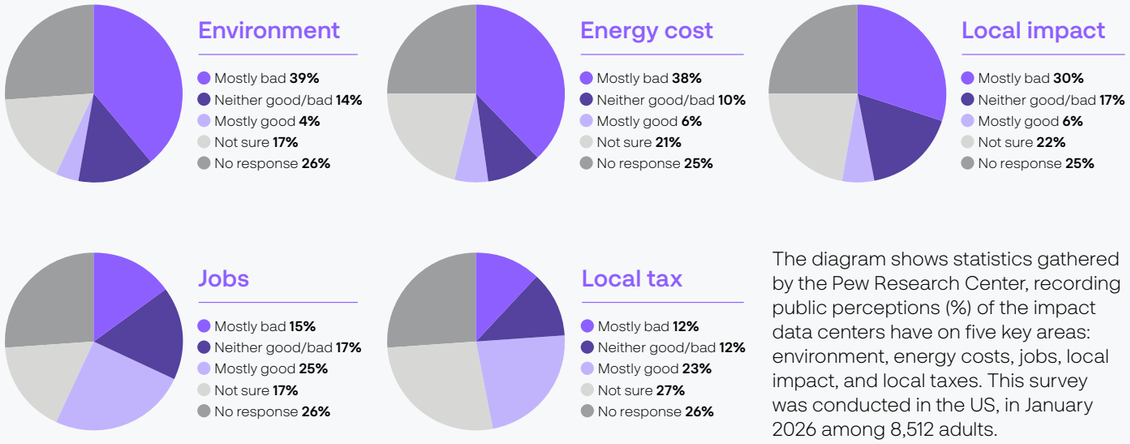
Western US Water consumption – water scarcity, chronic drought conditions, competing agricultural and residential water demands, public perceptions that tech companies are being prioritized

Midwestern US Land use and rural industrialization – conversion of farmland into industrial campuses, noise emissions, perception that tax incentives benefit corporations not the public, tension between rural identity and tech expansion

Northeastern US Energy use and grid strain – grid congestion, high electricity bills, concerns about backup generators, large hyperscale clusters

Southwestern US Water usage, air quality, and heat-driven grid instability – extreme heat waves stress the grid, water scarcity in desert regions, air-quality concerns from backup systems, rapid industrial growth

Southeastern US Environmental impact and land-use – strong activism culture, river ecosystems and hydropower strain, land-use conflicts in suburban and rural areas, opposition to diesel emissions in green regions



The diagram shows statistics gathered by the Pew Research Center, recording public perceptions (%) of the impact data centers have on five key areas: environment, energy costs, jobs, local impact, and local taxes. This survey was conducted in the US, in January 2026 among 8,512 adults.



Localized backlash & political pressure

Detail

Such backlash commonly manifests through grassroots campaigns that leverage social media to contest concerns at hearings and local council meetings, repeatedly demonstrating the ability to use open-source information to identify early signals, such as quiet land acquisitions and non-disclosure agreements by developers. Disruptions of this nature typically remain peaceful, limited to disrupting proceedings to voice objections and to sporadic use of posters and chants to further campaigns. Local mobilizations outside data center construction sites / already constructed data centers are comparatively rare, with the consultation period offering the only legal window where public input can change the outcome before permits are granted and zoning is finalized.

Statistics: $18 billion worth of data center projects were blocked and another $46 billion delayed between 2024-2025 following public opposition and activist targeting.

Backlash to data center development is bipartisan and serves as a national flashpoint in many countries, impacting local politics and laws while marking a unique discrepancy between local and federal / national standpoints; local authorities aim to represent residents' viewpoints while national governments remain pro-expansion, prioritizing geopolitical competition and economic strategy.

Case study Regional decisions in US

- Jersey City in New Jersey, US, banned data centers as the primary use of industrial property in July 2026.
- Nashville in Tennessee, US, passed strict zoning rules for data centers and a temporary moratorium on all new data center permits until 1 December in July 2026, stipulating requirements including the distance of data centers from 'sensitive locations', environmental restrictions, annual compliance reports, and public reporting on water and electricity consumption.
- Residents of Warrenton, Virginia, US, voted out all town council members who supported Amazon's proposed data center in the November 2024 election, replacing them with a newly elected council composed entirely of project opponents who moved to reject the prior approvals.

Case study National decisions in US

- US Environmental Protection Agency will not enforce the federal Clean Air Act's Acid Rain program, a pollution law that has been key to a dramatic reduction of smog and soot pollution from industrial facilities, on power sources only providing electricity to data centers, as per statements from July 2026.
- US President Donald Trump criticized New York's decision to enact a one-year statewide pause on hyperscale data centers in July 2026, calling it a "terrible decision" that should be reversed "immediately."
- The US Administration signed the Accelerating Federal Permitting of Data Center Infrastructure Executive Order in July 2025, allowing the lease of federal and military land for data centers.





Advisory

- Data centers will almost certainly continue to face a patchwork legal framework caused by competing legal and regulatory priorities across countries, highlighting the need for organizations to diligently assess existing and proposed laws and policies that could complicate operations.
- Organizations are advised to conduct community liaison measures prior to official requests to establish local views on a data center in the area to prevent possible backlash.
- It is advised that organizations strictly adhere to local regulations to mitigate legal repercussions and heightened local backlash.

Colocation and CNI dependencies

Bottom line up front (BLUF)

Data centers are becoming increasingly dependent on external infrastructure, whether through colocation or critical national infrastructure (CNI), because the sector's rapid expansion, driven by AI and cloud computing, demands unprecedented volumes of power and water that individual operators can no longer self-provision. Such dependencies are becoming a strategic decision rather than optional because of their scale, load, and resource intensity; however, this exposes data centers to the vulnerabilities of third parties.

Assessment

Threat level 3

Most likely course of action (MLCOA) vs Most dangerous course of action (MDCOA)

MLCOA: As the demand for data centers grows, colocation will likely become an increasingly attractive choice for economic purposes; however, risks when collocating, such as depending on third-party infrastructure and sharing a space with other entities, will likely persist. Further rapid expansion of data centers depending on CNI will likely inspire concerns regarding capacity and operational continuity, with grid strain and water scarcity possibly posing a long-term risk to data centers. Dependencies pose a complex security landscape for data centers, inspiring threats that are often out of the hands of operators.

MDCOA: Colocation becomes a favored option to curb the financial and zoning burdens for data centers, exposing more organizations to the risks associated with collocating. This is exploited by threat actors to disrupt operations and extract sensitive information, with limited oversight of security preventing organizations from aligning efficient security measures. CNI reliability decreases substantially, heavily impacted by extreme weather trends, increasing demand, and activist targeting, inhibiting the operational capacity of data centers, and forcing organizations to self-provision necessary power and water sources, increasing financial strain.

Detail

Data centers are increasingly shifting towards colocation models, in which organizations rent a physical space from a third party to house servers and computer hardware, thereby inheriting electricity, cooling, and security capabilities without the costs of private premises. While this affords a long-term economic advantage, the threat landscape will be shaped by the vulnerabilities and exposure of the premises and other collocating entities.



Security and access vulnerabilities

Colocation environments inherently broaden the number of individuals, contractors, and vendors who have legitimate access to the site. This increases the possibility of unauthorized access, whether that be by accident, through exploitation of weak controls, or social engineering.

- **Shared physical perimeters:** Multiple tenants rely on the same entry points, guard staff, and surveillance systems, meaning a breach of one tenant can expose others.
- **Multi-tenant access control systems:** Misconfigurations can allow cross-tenant access, with badge systems and biometric checkpoints needing to differentiate between tenants.
- **Tailgating:** High foot traffic from different organizations increases opportunities for unauthorized individuals to follow authorized personnel into restricted zones.
- **Vendor and contractor access:** Third-party maintenance often has broad access privileges, and weak vetting / inconsistent escorting policies can create exploitable gaps.
- **Network separation:** Digital infrastructure is often shared, allowing other tenants to serve as a man-in-the-middle (MitM) for cyber intrusions should they have lax cyber security measures.
- **Activist targeting:** Nearby / other collocating organizations that have major controversies can be at risk from activist targeting, of which collocating data centers could experience the indirect impacts of, such as restricted access from blockades, damaged assets from criminal damage / vandalism, and operational degradation from investigation processes.

Insider threats

An insider threat is any person who has / had authorized access to or knowledge of an organization's resources and uses this to intentionally or unintentionally harm equipment, facilities, personnel, information, systems, or resources. It is therefore irrespective of employment status and determined by the level of access and trust given to the individual, and includes current employees, former employees with residual access, third-party contractors, business partners, and temporary staff. Such risks increase in colocation environments.

Unintentional		Intentional / Malicious	Collusive	Third Party
Negligence	Accidental	Intentional actions that are taken to harm an organization for personal benefit or to act on personal grievance. This can include 'whistleblowers', who leak data on the grounds of public interest.	One or more insiders collaborate with an external threat actor to compromise an organization. Employees, sometimes referred to as 'pawns', are often targeted by external threat actors through social engineering or spear phishing campaigns.	Threats that arise from third parties, such as contractors or vendors, who have access to facilities.
Employees or contractors who expose an organization to a threat through carelessness. This is often due to a lack of training in security policies as opposed to ill intent.	An insider who mistakenly causes an unintended risk.			

Control and compliance

Tenants have low visibility and control over internal maintenance and third-party vendors, meaning many of the security decisions and much of the maintenance of premises lack the ideal oversight of collocating organizations to ensure it meets industry standards.

Dependence on CNI, such as power and water sources, further exposes data centers to inherited security and operational risks through single points of failure that threaten operational continuity and capacity.

- **Reduced resilience during extreme weather:** Heatwaves increase both electricity demand and water scarcity, simultaneously stressing cooling and power systems.
- **Grid instability exposure:** Voltage fluctuations or regional load-shedding can cause equipment stress and cascading shutdowns.
- **Regulatory drought measures:** Governments can impose usage caps during heatwaves, limiting cooling capacity.
- **CNI targeting:** CNI, such as power stations and water sources, is increasingly targeted by activists, notably political extremists, attempting to further their campaign through high-visibility and impactful actions that degrade commercial capacity and civilian life.

Case study

The far-left activist group, the Vulkangruppe / Volcano Group, set fire to a cable bridge at the Lichterfelde Heating and Power station in January 2026, resulting in power outages for ~40,000 households and ~2,200 businesses in southwest Berlin, with the outage taking ~four days to resolve. The action aimed to protest the use of fossil fuels within the energy sector, which is commonly protested against for its contribution to climate change. Fuel supplies started to diminish, mobile networks were disrupted, and care homes, schools, and hospitals were forced to relocate or limit / close services, with freezing temperatures also complicating the situation.



Advisory

- Before collocating, establish threat assessments for all other organizations on the premises, considering what exposure they bring to the site and how this could impact operations.
- Assess the reliability of CNI in the region, using this to decide location suitability, and establish contingency plans for possible outages.
- Compare the security posture of colocation sites to sector-specific standards, recognizing that limited oversight could hinder future collaboration to mitigate or prevent security breaches.

Key focus area 5

Supply chain volatility

Bottom line up front (BLUF)

Supply chain volatility in the data center sector is increasingly shaped by geopolitical pressure, sanctions regimes, organized crime activity, and targeted theft of critical components. These interact with existing manufacturing bottlenecks to create a more complex and security sensitive risk environment than traditional procurement models.

Assessment

Threat level 3

Most likely course of action (MLCOA) vs Most dangerous course of action (MDCOA)

MLCOA: Supply chain volatility will continue, with geopolitical flashpoints serving to impact supply chain continuity and the rapid increase of value within the sector inspiring OCG / opportunistic theft. This will become more noticeable as demand grows, and see incremental increases in the costs of infrastructure materials needed for data center construction.

MDCOA: Data center materials become a central strategic target for nation states to further geopolitical and market goals, lengthening the time it takes to build data center infrastructure and creating further supply bottlenecks. High-value components necessary for data center operations incite increased OCG / theft targeting, with established networks focused on such goods, sporadically moving to steal assets from operating data centers.



Supply chain volatility

Detail

Sanctions, notably those affecting metals, semiconductors, and electrical grid equipment, disrupt production and redirect global flows of copper, steel, and transformers. When major producing states face export controls or geopolitical isolation, downstream operators experience unpredictable lead times, sudden price shocks, and constrained access to essential infrastructure.

Case study China

China's sanctions on critical minerals have created upstream constraints that slow US data center development by disrupting supplies of electronics materials and rare earth components. These controls emerged through a tit for tat dynamic, with China responding to successive US semiconductor export restrictions and entity list actions by weaponizing its dominance in upstream minerals. The pattern reflects broader geopolitical competition, where both states target strategic chokepoints central to AI rather than simply trying to degrade commercial markets.

Sanctions also reshape illicit markets, creating incentives for organized crime groups (OCGs) to exploit shortages and regulatory gaps. When legitimate supply chains tighten, criminal networks often fill demand through theft, diversion, counterfeiting, or gray market distribution of high value components. Transformers, generators, copper cabling, and specialized cooling equipment have become attractive targets because they can be resold across borders with minimal traceability. OCGs operating in regions with weak enforcement exploit these dynamics, moving stolen equipment through transnational logistics routes that mirror narcotics and commodity smuggling pathways. This activity increases procurement risk for data center operators, who may unknowingly encounter compromised or counterfeit components that undermine reliability and safety.

Case study Illinois

The Cook County Police Department in Illinois, US, recovered two trailers with $1.3 million worth of stolen data center supplies at a Chicago, US, truck yard in June 2026. This is a notable example of a strategic shift away from traditional consumer retail cargo theft toward high-value technology assets driven by the growth in the data center sector.

Theft and diversion of critical materials further amplify volatility by introducing operational uncertainty and degrading resilience. Copper theft has escalated in regions experiencing economic stress or sanctions driven scarcity. Stolen cabling, conductors, and grounding materials disrupt construction timelines and create vulnerabilities in electrical systems. In some markets, theft of generators, UPS units, and switchgear assemblies has been documented, reflecting the rising black market value of grid supporting equipment. These losses not only delay projects but also force operators into reactive procurement cycles, increasing exposure to inflated prices, unreliable suppliers, and extended lead times.



Advisory

- Monitor the progression / regression of international geopolitical tensions revolving around data center and AI market competition to preempt the direction of sanctions, using this to inform incident response plans (IRPs) and alternative supply sources.
- Liaise with local and regional police and intelligence authorities to facilitate information sharing about existing / emerging OCGs / theft trends that could pose a threat to data centers.
- Maintain situational awareness of OCG and theft patterns in proximate areas that could be displaced into areas of operations if apprehended by authorities.

Visit our website
to learn more

Contact

intelligence.solutions@securitas.com