The Brazilian Critical Infrastructure Threat Landscape and Implications for Healthcare Organizations

TLP:WHITE This report may be shared without restriction. For Health-ISAC Members be sure to download the full version of the report from the Health-ISAC Threat Intelligence Portal (HTIP). Contact Membership Services for assistance.

Health-ISAC™ Collaborating for Resilience in Healthcare

RANE Risk Assistance Network + Exchange

Key Judgements

- Fragmented care between rural and urban clinical environments has led to heightened risks of violence toward health sector employees. Brazilian centralized healthcare access requires large data stores, which threat actors have often targeted.
- Nation-state actors and financially-motivated criminals pose espionage, data breach and extortion risks: Brazilian critical infrastructure organizations face a broad array of cyber threats, including sophisticated foreign state-sponsored threats, as well as growing nonstate cybercriminal (and hacktivist) campaigns, which elevate a range of monetary and operational risks, including for healthcare entities.
- Petty criminals and organized criminal groups occasionally threaten critical services: Copper cable thefts are pervasive and sporadically result in blackouts or disruption to traffic light systems, while organized criminal groups damage or prevent maintenance of water stations and telecommunication antennas in low-income areas they control, posing operational risks to healthcare service providers in these regions.
- Protest activity and labor action will likely pick up ahead of 2026 elections: Brazil's polarized political and social environments will fuel recurring protests and strikes over the coming 18 months, opening the door to sporadic violent and/or disruptive incidents.
- Terrorism risks will remain low, although isolated plots will persist: While Brazil has not recorded terrorist incidents in recent decades, police have thwarted multiple plots in recent years, highlighting underlying risks of religiously- or politically-motivated attacks.
- Increasingly frequent extreme weather events threaten to disrupt transportation and utilities: Intense droughts have become more frequent and will threaten hydroelectric power generation and water transportation, while heavy rains will result in flash floods and landslides, causing significant damage to urban and road infrastructure.

Brazil Threat Landscape

Numerous threat actors pose a range of risks for critical infrastructure entities in Brazil, including sophisticated cyberespionage groups linked to foreign governments, chiefly China and, secondarily Russia. Brazil's digital landscape has expanded significantly in recent years, accelerated by Brasilia's enthusiastic embrace of digital platforms like the federal government's gov.br portal launched in 2019 and the Pix digital payment system introduced in 2020. While this has brought benefits, Brazil's expanding digital landscape has also broadened the country's attack surface, a trend worsened by the government's lax cybersecurity rules and weak enforcement.

As a result, organizations operating in Brazil are exposed to a variety of digital threats, the most critical of which stem from state-sponsored groups linked to other countries, namely China and, secondarily, Russia. While Brazilian President Luiz Inácio Lula da Silva maintains positive relations with both Beijing and Moscow – and has sought to expand economic partnerships with both countries and diplomatic cooperation via the BRICS+ bloc – they nevertheless both have a concerted interest in expanding their influence in Brazil. This is especially true of China, which has pursued several investment projects in Brazil's critical infrastructure sectors, particularly the electricity, energy, technology and telecommunications industries.

In line with its offensive threat activities elsewhere, Chinese state-sponsored actors often seek to leverage private sector partnerships to gain internal access to critical infrastructure networks to monitor and collect intelligence or intellectual property. While strategic government agencies (defense, intelligence, etc.) are likely to be the biggest target of such campaigns, private sector entities with links to Brazil's government, such as via contracts, may be more vulnerable to Chinese-linked state-sponsored campaigns. In the healthcare industry, Brazil and China have similarly maintained close collaboration around research and other joint initiatives, indicating that Chinese threat groups could similarly seek to occasionally make inroads into healthcare-linked organizations, though likely only for nondisruptive IP theft. Russian state-linked groups similarly pursue cyberespionage and influence campaigns targeting Brazil's cyberspace, though the Kremlin's resources have been more constrained since the outbreak of the Russian-Ukrainian war and likely focus more exclusively on strategic government entities.

- While Brazil is not a member of the Belt and Road Initiative, several Chinese companies have pursued expansive investment projects in the country. For example, Chinese telecommunications company Huawei has been integral to Brazil's digital infrastructure development for almost a decade. The State Grid Corporation of China has also funded numerous high-voltage transmission projects for clean energy sources.
- Brazil's healthcare sector has embraced digital infrastructure for various patient services, exposing healthcare entities to digital compromise. Certain private companies are highly prominent digital service providers which offer diagnostic solutions to healthcare facilities in more than 200 Brazilian cities. In June 2024, the Brazilian Oswaldo Cruz Foundation – one of Brazil's most prestigious science and research institutions – announced a joint initiative with the Chinese biopharmaceutical company Sinovac which pledged a $100 million investment in the country for vaccine and cell therapy research and development following a close partnership to produce COVID-19 vaccines during the pandemic. The two organizations also announced their intention to bolster joint research through BRICS+ vaccine R&D center, which was established in March 2022.

Cybercriminal Landscape

Beyond foreign state-sponsored actors, nonstate cybercriminals and hacktivists have also become a more pronounced threat in Brazil in recent years, with the former posing significant financial and operational risks for vulnerable organizations – including, critical infrastructure entities – while the latter still primarily conduct low-sophistication and short-lived cyber campaigns. Beyond foreign state-linked threats, cybercriminals are likely a more relevant threat as Brazil's weak enforcement action against illicit digital groups has resulted in the rise of a variety of domestic cybercriminal syndicates that regularly target domestic and international entities alike based on the opportunistic likelihood of receiving a financial payout. While Brazil has become particularly notorious for a broad range of homegrown banking trojans, which primarily affect financial account holders, cybercriminals have also pursued more sophisticated ransomware attacks that have impacted private and public sector entities alike (including repeated hacks against Brazilian government ministries), as these groups seek out organizations across industries that have weak cybersecurity defenses and present an opportunity for extortion.

Financially-motivated threat actors are often more enticed to target sectors that have a higher impetus to avoid operational disruptions, which is what makes the healthcare sector attractive because patients may need critical and immediate life-saving services. Brazil has also witnessed an influx of hacktivism as independent politically-motivated groups have become more pronounced in the wake of foreign crises ranging from the Russian-Ukrainian war to the Israel-Hamas war. While Brazil has not been directly impacted by these crises, Brazilian organizations have occasionally been caught in the crosshairs of hacktivist activity, although these groups typically rely on low-level tactics like distributed-denial-of-service (DDoS) and website defacement campaigns. A more localized hacktivist risk stems from the environmentally-motivated Latin American group Guacamaya, but it primarily targets extractive industry companies like miners and oil and gas firms.

Criminal Landscape

Criminals often steal metallic cables that disrupt the power supply, while organized criminal groups have sought to disrupt telecommunications and utilities services, threatening facilities operating in areas under criminal control. Brazil experiences high levels of both violent and nonviolent crimes, with higher violence levels usually concentrated in marginalized portions of large cities, such as Rio de Janeiro and São Paulo, and in northern and northeastern states. Specialized gangs and petty criminals often steal metallic components, with preferred targets including copper cables, which are broadly used for public lighting or transportation services, such as metropolitan trains. Recurring thefts often disrupt urban railway services, especially in the Rio de Janeiro metropolitan area, or cause gridlock, as they impede the adequate functioning of traffic lights and could eventually cause blackouts. Occasionally, criminals inadvertently damage fiber optic cables when trying to steal metallic components, resulting in the interruption of phone or broadband services as well.

eventually cause blackouts. Occasionally, criminals inadvertently damage fiber optic cables when trying to steal metallic components, resulting in the interruption of phone or broadband services as well. In areas under organized crime control, especially in the outskirts of the Rio de Janeiro metropolitan area and, to a lesser extent, in low-income neighborhoods in other state capitals, criminal groups have prevented telecommunication companies from carrying out regular maintenance work. The deterioration of antennas and other equipment occasionally results in the interruption of phone and data coverage services over time, which criminals then leverage to force local residents and businesses, including hospitals or healthcare service firms, to resort to them as providers. Criminals adopt similar tactics to hurt water provision, by stealing or damaging cables or pumps used in water treatment stations. In addition to operational challenges poor telecommunication or the interruption of utilities services could pose, directly or indirectly hiring criminal organizations as utilities or service providers could also pose compliance and reputational risks to healthcare companies with operations in these areas.

- A cable theft incident left the Paranoa Regional Hospital, in Brasília, without power on March 19, 2025, with media reports indicating that the blackout led to the worsening of some patients' clinical conditions, including babies.

Political Factors

Political unrest in Brazil occurs semi-regularly and sometimes creates disruptions for critical infrastructure, and these threats will likely rise over the next year-and-a-half due to elevated political tensions. Brazil experiences moderate levels of unrest, as while protests occur frequently in major cities such as Rio de Janeiro, São Paulo and Brasília, the majority are non-violent and short-lived. In recent years, the country has experienced semi-regular political protests both supporting and opposing former President Jair Bolsonaro.

In 2025, supporters of Bolsonaro have launched multiple mass protests over criminal charges against him in relation to his alleged involvement in the coup d'etat plot intended to keep him in office following the October 2022 presidential election. Though protests have not reached the scale of damage caused on January 8, 2023 – when Bolsonaro supporters attacked government buildings in Brasilia – protests have seen tens of thousands participate. Left-wing groups against Bolsonaro also protest in support of democracy and President Lula da Silva, with additional sporadic protests in response to unpopular political developments. There is the high likelihood that unrest risks will increase over the next 18 months, with protests likely in response to major developments in the multiple cases against Bolsonaro and particularly if he is convicted and/or arrested. Brazil's 2026 elections will also be a likely flashpoint for unrest, as the political divisions seen during the 2022 presidential election persist and will likely trigger in regular demonstrations that sometimes include violence. Protests occasionally block major roads, preventing critical infrastructure and healthcare sector workers from transiting the area. Political protests in Brazil generally do not specifically target critical infrastructure, but extremists have conducted politically-motivated attacks.

- Following the 2022 presidential election, truck drivers blocked hundreds of roads across the country for several days, causing shortages of fuel and goods as Brazil relies on road transportation for two-thirds of the goods it produces and consumes.

Labor Strikes

Brazil frequently experiences strikes and labor rights-related demonstrations, which occur across various sectors, but especially among transportation workers, oil and gas workers, teachers and government employees. Such strikes will likely become more common over the coming years as broader economic frustrations make workers more willing to strike. The majority of strikes in Brazil are peaceful, but they often create disruptions amid efforts to block access to critical infrastructure including power stations, transportation nodes such as airports and seaports, and major roads, reduced staffing, and, in some instances, damage to facilities. Localized health sector strikes occur sporadically (though nationwide strikes have previously occurred), and can be particularly disruptive for medical organizations because such labor actions have previously delayed elective health services and blocked access to health facilities. Strikes by electricity workers also risk disrupting energy supplies, forcing health facilities to use more expensive and less reliable generators to remain operational. Popular discontent with the quality of public health services, which in some cases are performed by private sector contractors, have also led to mostly peaceful protests or rage incidents in healthcare units across the country.

- In 2024, workers at Brazil's environmental enforcement agencies launched a months-long strike, during which they halted fieldwork in order to protest low wages and poor working conditions. Disruptions included the slowing of oil and gas permit approvals, halted work on electricity facilities, and delays to vehicle imports.
- While there have not been major nationwide healthcare strikes in Brazil in recent years, a 2011 physicians strike by at least 120,000 doctors over low wages and interference by health insurance companies disrupted elective medical care. The strike reportedly impacted between 25 and 35 million Brazilians. More recently, in March 2025, public sector workers including some medical workers went on strike for multiple days in Poços de Caldas municipality, Minas Gerais state, to demand wage increases.
- Brazilian doctors have also carried out protests to oppose the "Mais Medicos" government program implemented in 2013, which employed Cuban doctors to offset the shortage of physicians in isolated areas of the country. The resumption of similar policies could lead to the reemergence of demonstrations targeting healthcare companies or units associated with the initiative.

Terrorism

Terrorism concerns in Brazil are low despite multiple terrorist plots and non-deadly politically-motivated attacks in recent years, posing minor risks to critical infrastructure. Brazil experiences low terrorism levels, with no terrorist groups maintaining a significant presence in the country. Some terrorist groups have a presence in the tri-border area with Argentina and Paraguay, including the Iran-backed transnational terrorist group Hezbollah. Still, some violent extremist incidents have occurred in Brazil in the last three years.

Brazil is experiencing elevated terrorist risks against Jewish targets related to the Israel-Palestine conflict, demonstrated by a thwarted attack plot against synagogues in 2023, as well as the arrest of an Islamic State member attempting to recruit Brazilians in 2024. However, Islamist attack plots made public have not previously targeted infrastructure. Political extremists have also conducted physical but non-deadly attacks in Brazil in recent years, including a bomb explosion outside the Supreme Court building in Brasilia in November 2024 and a foiled bomb attack on a tanker near Brasilia's airport in December 2022. Finally, Brazil is facing low but rising threats from online youth radicalization. Demonstrating this threat, Brazilian police thwarted a bomb plot targeting a Lady Gaga concert on May 3, 2025, in Rio de Janeiro, which allegedly sought to target LGBTQ+ people and give the perpetrators notoriety on social media. However, there is no indication that there is a high risk of similar plots, and overall, any terrorist violence that disrupts critical infrastructure is likely to be localized and short-lived.

Extreme Weather

Increasingly frequent extreme weather events will continue to damage infrastructure, disrupting power and water provision and interrupting traffic in cities and major roads, while occasionally threatening electricity generation. In recent years, Brazil has experienced an increased number of intense droughts and severe storms exacerbated by the El Nino and La Nina weather phenomena, leading to significant impacts on infrastructure and resources. Various cities, including state capitals across the country, experience elevated risks of flash floods and landslides on the back of heavy storms during the rainy season that usually runs from November to April. Large rainfall volumes usually damage asphalt in urban centers, cause landslides in low-income residential areas, block roads and eventually cause the collapse of bridges.

Governments' limited fiscal capacity and often uncoordinated response mean that in some cases repairs can take several weeks or even months, translating into operational challenges, disruption to supply chains or elevated costs to ship supplies through alternative routes. Heavy rains with strong winds also tend to topple trees and damage power lines at urban centers and transmission structures in rural areas, resulting in blackouts, posing risks to healthcare facilities that do not rely on external power generators. Increasingly frequent severe droughts have also impaired water provision, waterway transportation and power generation, especially as Brazil relies on hydroelectric power for nearly 60% of the electricity it consumes. Although water and electricity rationing measures have only been adopted in extreme circumstances (such as in 2001 and 2014), droughts have led the government to prioritize the use of water for electricity generation over grain shipment and resort to thermal power plants, increasing electricity costs. Extreme droughts also significantly disrupt transport in the Amazon region, which heavily relies on rivers for cargo and passenger transportation. Wildfires on the back of a dry climate have also threatened power lines and overwhelmed healthcare facilities in various regions.

Health Sector Impacts

The threat landscape in Brazil contains numerous threats to both the physical security of health sector facilities and the networks protecting Brazilian protected health information (PHI).

Physical

Various systemic factors have led to a state of increased physical security risk for health sector facilities and employees in Brazil. One of the major drivers of this state is the difference in levels of care from rural regions to urban areas, with more advanced and specialized offerings available in urban areas as opposed to rural areas. The shortage of specialized medical professionals further exacerbates this fragmentation. As a result, facilities that offer advanced or specialized care may be at higher risk of workplace violence incidents involving altercations with disgruntled patients as they experience an influx of patients from surrounding rural areas. To learn more about how to minimize the risk of workplace violence in care delivery environments, please read the Health-ISAC white paper on Behavioral Incident Response Strategies in Clinical Settings here.

Cyber

In Brazil, access to healthcare is a constitutional right. To make sure citizens exercise this right, the Brazilian Government operates a national healthcare service model, the Unified Health System (SUS), where access to care can be centralized. These large, centralized data stores have become a target for threat actors in the Brazilian health sector threat environment. Database security is likely to be a frontline security issue for Brazilian health sector entities. Data breaches that include patient PHI can represent significant reputational damage for the individual care-providing organizations and its parent companies providing services both in Brazil and abroad.Health-ISAC recommends taking the following measures to reduce the risk of data breaches:

- **Audit user permissions** to ensure employees only possess the privileges that allow them to access the data that is necessary for their role, avoiding privilege creep. This measure will reduce the access a threat actor would have in the event that a low-privileged account became compromised.
- **Storing data in encrypted form to reduce exposure in the event of data exfiltration**. This measure reduces the risk of reputational damage in the event of a data breach because the data exfiltrated would not be in plaintext form, making it much harder to operationalize.
- **Implement input validation measures on public-facing data portals**, reducing the risk of structured query language (SQL) injections. This measure will reduce the risk of data exfiltration and tampering.