

Four Key Threats to Critical Infrastructure

Building resilience in an increasingly
interconnected world

APRIL 2026

Welcome to Spotlight — presenting insights, shifting perspectives and reframing evolving global trends.

Presenting the issues, opportunities and risks that are transforming the way we do business, from industry hot topics and emerging growth markets through to perspectives on the big questions shaping our world today, this article provides actionable insights and analysis to inform strategic decision-making and power onward growth plans.

The Spotlight content series is designed for company executives, risk managers, industry operators and business owners looking to reframe pressing issues, shape strategy and pursue their future ambitions with confidence.

Key insights

1

Converging pressures of geoeconomic confrontation, cyberthreats, extreme weather and aging systems are causing disruptions to critical infrastructure and amplifying risks across physical, cyber and cyber-physical systems (integrating digital algorithms with physical systems).

2

Cyber attacks targeting critical infrastructure continue to escalate as state-sponsored actors move beyond data theft to pre-position capabilities inside essential systems. Meanwhile, AI is being weaponized to generate malware and conduct phishing campaigns at scale.

3

Ransomware remains the most feared cyberthreat among Chief Information Security Officers (CISOs) globally, with attacks on the US telecommunications sector increasing fourfold since 2021 and mostly compromising the critical infrastructure in the region's private sector.

4

Natural catastrophes and extreme climate are inflicting growing damage on essential systems. Significant impacts include transformer failures and power disruptions, while cyclones and wildfires are exposing the limits of infrastructure built for a more stable climate.

5

Aging and chronically underfunded physical infrastructure represents a mounting systemic risk. The 2025 Calgary main breakage that served nearly two-thirds of the city's water supply is a warning that deferred maintenance doesn't reduce risk; it concentrates it.

Disruptions to critical infrastructure have risen four positions among the top risks, from rank 26th to 22nd in 2026, in the two-year outlook of the World Economic Forum's Global Risks Report, reflecting a sharp increase in global concern.¹

Today, we rely on physical infrastructure systems more deeply than most people ever pause to consider. The intricate networks of essential systems — including energy, water, transportation and communication — ensure the seamless operation of our communities, healthcare systems, economies and governments.

As our reliance on these systems deepens, so does our vulnerability to the multitude of emerging threats that can compromise their stability, safety and integrity. Four converging pressures are making critical infrastructure increasingly fragile:

1. Geoeconomic confrontation is amplifying threats to critical infrastructure across physical, cyber and cyber-physical systems alike.
2. Frequent and intense extreme weather, from floods and wildfires to extreme heat and drought, are directly damaging infrastructure and permanently altering the environments it was built to serve.
3. Cyber attacks on critical infrastructure are intensifying. The digitalization of essential systems creates new vulnerabilities that malicious actors, particularly from organized criminal groups to state-sponsored operators, are actively and systematically exploiting.
4. Aging systems spanning transport networks, power grids and water systems across the Organization for Economic Co-operation and Development (OECD) countries now face costly maintenance burdens. This comes at a time when debt-constrained governments are least able to fund them.

With smart cities and digital economies reshaping modern living, the transformation of critical infrastructure has reached a point where a single failure can cascade into economic disruption, public safety crises and geopolitical consequences.

The threat landscape has evolved just as dramatically. Where accidents and natural disasters once defined the primary risk to infrastructure, today's adversaries are deliberate, sophisticated and increasingly state-sponsored — with cyber intrusions and acts of political aggression now taking center stage.

In addition to these evolving threats, other factors such as aging infrastructure and a lack of investment in its improvement contribute to the vulnerability of critical infrastructure. Over time, structures have deteriorated, slowly becoming weakened and susceptible to failure. One example is the crumbling concrete problem currently affecting many public buildings in the UK, prompting the UK government to allocate hundreds of millions to fix the issue.²

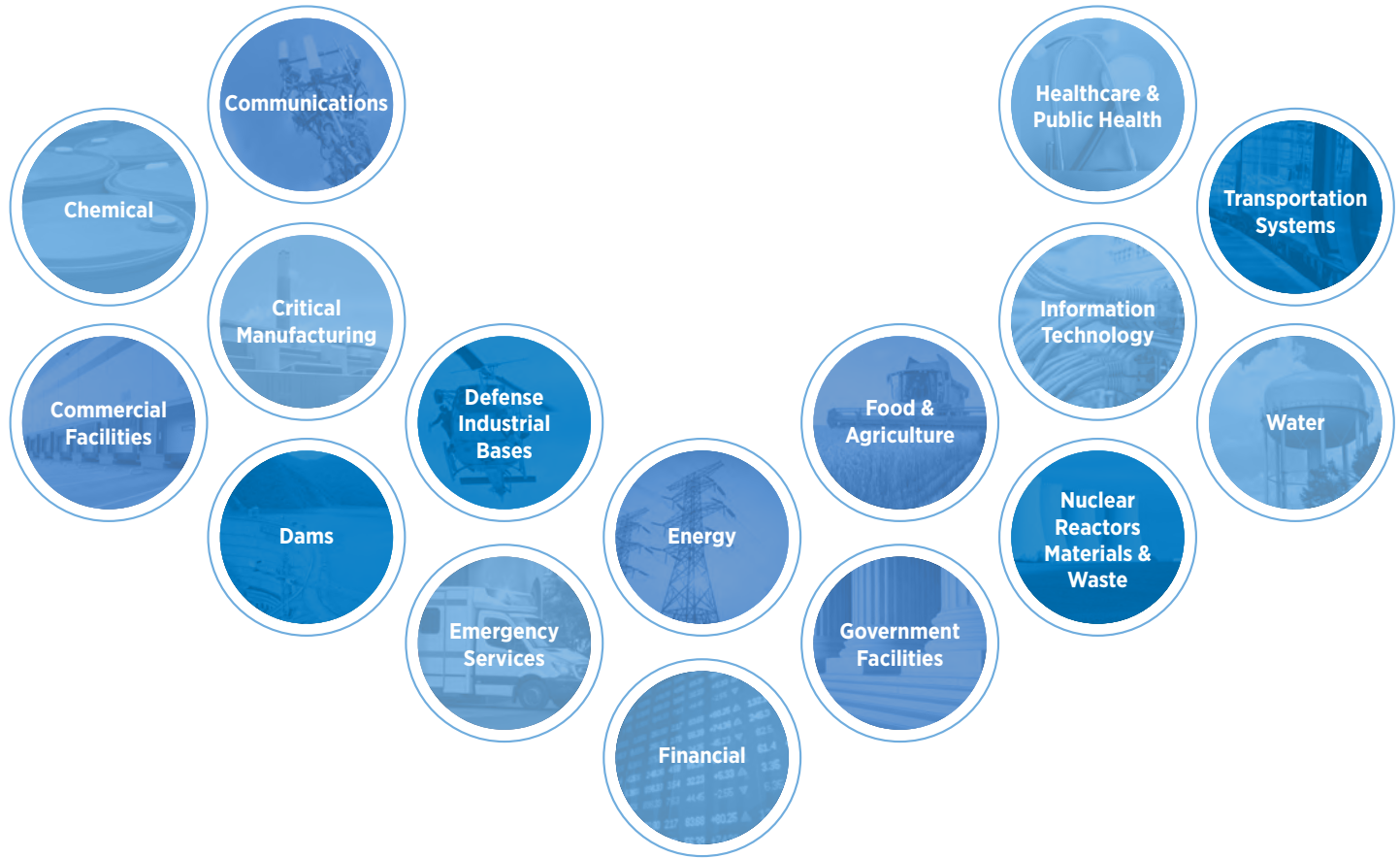
Further, the complexity of the diverse demands of our critical infrastructure systems has the potential to overwhelm legacy IT systems. Threat actors are exploiting these vulnerabilities to compromise essential services.

Gartner has warned that misconfigured AI in cyber-physical systems could pose a risk of large-scale disruption to national critical infrastructure in a G20 country by 2028.³

The four major threats to critical infrastructure are not isolated, working in tandem with other macro-trends, including urbanization, population growth, climate change and digitization, to exacerbate the exposures faced by critical infrastructure.



Critical infrastructure sectors



Source: Cyber and Infrastructure Security Agency



1. Geopolitical risk

Geopolitical risk looms large as a pervasive threat, often the product of the interplay between political, economic and security fractions within and between nations. It encompasses a broad spectrum of factors, from intergovernmental conflicts and trade disputes to territorial and ideological tensions that adversely affect the critical infrastructure of the involved region.

Threats to critical infrastructure

- **Trade disruptions**

Regional geopolitical tensions, influencing the supply chain through sanctions, tariffs, embargoes or trade wars, can make infrastructure vulnerable to sudden disruptions. This in turn can create dependence on specific regions for essential goods and services, leading to delays, shortages and rising prices almost overnight.

- **Physical attacks and terrorism**

Attacks on critical infrastructure are often fueled by geopolitical and ideological differences. Attacks on power plants, airports or transportation networks can lead to prolonged economic consequences.

- **New policies**

Tensions between regions can lead to changes in trade agreements, investment or data privacy policies, imposing greater compliance requirements on critical infrastructure operators. Unforeseen regulatory changes can affect market prices, disrupt operations and impede investments.

- **Cybersecurity breaches**

State-sponsored cyber attacks have become a significant arrow in the espionage quiver for countries seeking to disrupt, sabotage or exert control over vital infrastructure systems.

- **Wartime focus on critical infrastructure**

Targeting critical infrastructure, especially those in the energy sector, has become a defining tactic of modern conflict. For instance, the 2026 Middle East conflicts caused international shipping to come to a standstill at the entrance to the Strait of Hormuz, through which about 20% of the world's oil and gas is shipped.⁴ Additionally, power grids and the electrical distribution substations remain particularly vulnerable as they're often remotely located and difficult to defend, making them targets for attack.

Severed connections: The threat to undersea infrastructure

The Baltic Sea cable attacks — weaponizing connectivity in hybrid conflict

A sustained pattern of damage to the Baltic Sea's undersea telecommunications, gas pipelines and energy cables has exposed the vulnerabilities of the physical infrastructure that links nine countries with shores along the region.

The incidents began with the 2023 damage to the Baltic connector gas pipeline and adjacent data cables between Finland and Estonia. Following this, on November 17, 2024, the BCS East-West Interlink, a 218-kilometer cable linking Sweden's Gotland Island to Lithuania, was severed.

Operators confirmed that this was not partial damage but a complete cut, **instantly eliminating approximately one-fifth of Lithuania's total internet capacity. Within 24 hours, the C-Lion1 cable connecting Finland and Germany was cut in the same region**, which was Finland's only direct submarine data link to continental Europe.

On Christmas Day 2024, the Estlink 2 electricity cable between Finland and Estonia suffered further damage, when a tanker, Eagle S, linked to sanctions-evading networks, allegedly dragged its anchor across the seabed for approximately 90 kilometers, **cutting five submarine cables in a single passage**. The Estlink 2 remained out of service for more than seven months, with repair costs reaching up to USD70 million.⁵

The cumulative toll is stark. **Since 2023, at least 11 underwater cables in the Baltic region have been damaged, with seven incidents concentrated between November 2024 and January 2025 alone.**⁶ Across these events, internet latency increased by 20% to 30% of measured network paths in the affected countries, as traffic was forced onto longer, slower alternative routes.

An attack on infrastructure that carries power, data or gas can sever the communications, energy supply and economic connectivity of entire nations, with consequences measured not in hours but in months, and with accountability that may never be fully established.

“A major concern is that we’re lagging behind when it comes to infrastructure resilience between countries, and a lot of that is under sea. Europe is going to become increasingly reliant on undersea electricity cables to North Africa, for example, and the Russian capability in this area is significantly ahead of ours. So that’s a good example of where we’re trying to play catch-up.”

— **Adam Carrier**, Head of Consulting at AnotherDay,
A Gallagher Company

Both physical and digital infrastructures bring significant challenges for defense, which are further complicated by the difficulty of attributing cyberattacks to a specific group or state. These intricacies impede effective counteractions and can erode confidence in the country’s capacity to neutralize such threats.

In the future, as battle lines are drawn in the fight for precious resources, new geopolitical exposures could arise. Rapid population growth and urbanization amplify the ever-increasing demand for resources such as water, minerals, energy and arable land. They can cause rising tensions between countries, with critical infrastructure likely to be amongst the collateral damage.

2. Natural catastrophes and extreme climate

Natural disasters and extreme weather can wreak havoc on essential systems, as recent history has shown. As climate scientists anticipate an increase in the frequency and severity of certain natural perils, this exposure is likely to remain significant, particularly for infrastructure assets in catastrophe-prone regions.

The January 2025 Palisades and Eaton wildfires in the Los Angeles area stand as the most economically destructive climate disaster of 2025, and among the costliest in recorded history.

The damage surpassed USD60 billion, with the fires claiming 31 lives directly, but the true human toll proved far greater. Approximately 400 additional deaths were attributed to secondary consequences of the fires, including prolonged exposure to degraded air quality and disrupted access to healthcare services.

Geomagnetic storms caused by solar flares in the Earth’s upper atmosphere have the potential to induce power in long conductors on the Earth’s surface, such as power lines, and overload electric grid systems, causing voltage collapse or damage to equipment. While remote, an event of such proportions can have catastrophic, long-term economic consequences, including blackouts and high maintenance costs.



The Gannon geomagnetic storm and the vulnerability of modern power grids

The Gannon geomagnetic storm of May 2024 is a sobering reminder that the threats facing critical infrastructure don't always originate on Earth.

Between May 10 and 12, 2024, at least five interplanetary coronal mass ejections arrived at Earth in rapid succession, producing the strongest geomagnetic storm in over two decades. It was the first to reach a **G5 or "severe" classification of geomagnetic storms**⁸ since October 2003 and was the most intense in terms of ground-level magnetic disturbance.

The storm's effects on power infrastructure were immediate and geographically wide-ranging. In southern Sweden, **geomagnetically induced currents penetrated the high-voltage transmission network**, causing disturbances in a transformer, resulting in a measurable drop in power supply along the interconnection linking Sweden and Poland.⁹

Strong induced currents were recorded in transformers in New Zealand and in the United States. In New Jersey, a 500 kV transformer at the Salem Nuclear Generating Station failed under the stress of geomagnetically induced currents. Auroras, ordinarily confined to high latitudes, were recorded as far south as the Tropic of Capricorn in Australia and across Mexico – a vivid illustration of the **storm's extraordinary global reach**.

What distinguishes the Gannon storm from its predecessors is that it didn't strike an analogue grid, but a modern, digitized one. Unlike the 1989 Quebec geomagnetic storm, which collapsed a power grid in less than two minutes, **the G5 storm tested the resilience of interconnected smart infrastructure**, exposing the extent to which high-latitude grids remain highly vulnerable to solar-induced currents. This event served as a stress test for modern digitized grids, causing transformer disturbances and power flow drops in Northern Europe (Sweden-Poland link).

The intensifying force of climate events were also made very real in Northern Vietnam on September 7, 2024, when **Super Typhoon Yagi** struck the country as the strongest storm in 30 years and the first violent typhoon of the 2024 Pacific typhoon season. Intensifying by eight levels within a single 24-hour period and retaining wind speeds exceeding 118 km/h at landfall, the storm defied typical weakening patterns, overwhelming infrastructure across the region.

The consequences for critical systems were immediate and extensive. Nearly **237,000 homes were destroyed or damaged**, and supply chains across key manufacturing corridors came to a halt. Across the wider region, spanning Vietnam, China, Myanmar, Laos, Thailand and the Philippines, **the total economic losses exceeded USD16 billion**.¹⁰

As climate change continues to intensify the speed, scale and unpredictability of storm systems, the infrastructure gaps it exposes today will only widen tomorrow. This makes investment in climate-resilient critical systems not a long-term ambition, but an immediate necessity.



3. Cyber threat

Before the advent of digital technology and the Internet of Things (IoT), the majority of our essential infrastructure was primarily physical. Now, a sizable portion of it has either moved online or is designed to be connected to larger IT systems.

As a result, critical infrastructure — including power grids, water supplies and transportation networks — is now vulnerable to cyberattacks that attempt to disrupt essential systems and cause extensive harm. The number of cyber attacks targeting critical infrastructure has increased significantly, along with their adverse effects on public safety, economic stability and national security.

Cyberattacks on critical infrastructure consist of various sophisticated techniques engineered to exploit particular vulnerabilities within networks, software and devices. These include **distributed denial of service (DDoS) attacks, malware and ransomware, phishing attacks, insider threats, advanced persistent threats (APTs) and physical attacks on cyber components.**

AI-driven phishing

Among the most concerning developments in this escalating threat landscape is the **growing use of AI to supercharge attacks on critical infrastructure.**

A recent instance occurred in February 2026, when the UAE Cyber Security Council announced that national cyber defenses had successfully thwarted a coordinated campaign of terrorist cyberattacks targeting the country's digital infrastructure and vital sectors.¹¹ The attacks combined **network infiltration attempts, ransomware deployment and AI-powered phishing operations** designed to harvest credentials and destabilize essential services.

What distinguished the campaign was not merely its ambition, but its method. By exploiting AI to generate highly convincing phishing content at scale, the attackers demonstrated how advanced offensive tools are now accessible to extremist organizations operating well below the threshold of state-sponsored cyber programs. The UAE's defenses — operating around the clock through cooperation among national agencies, service providers and international partners — detected and blocked the threats before any disruption occurred.

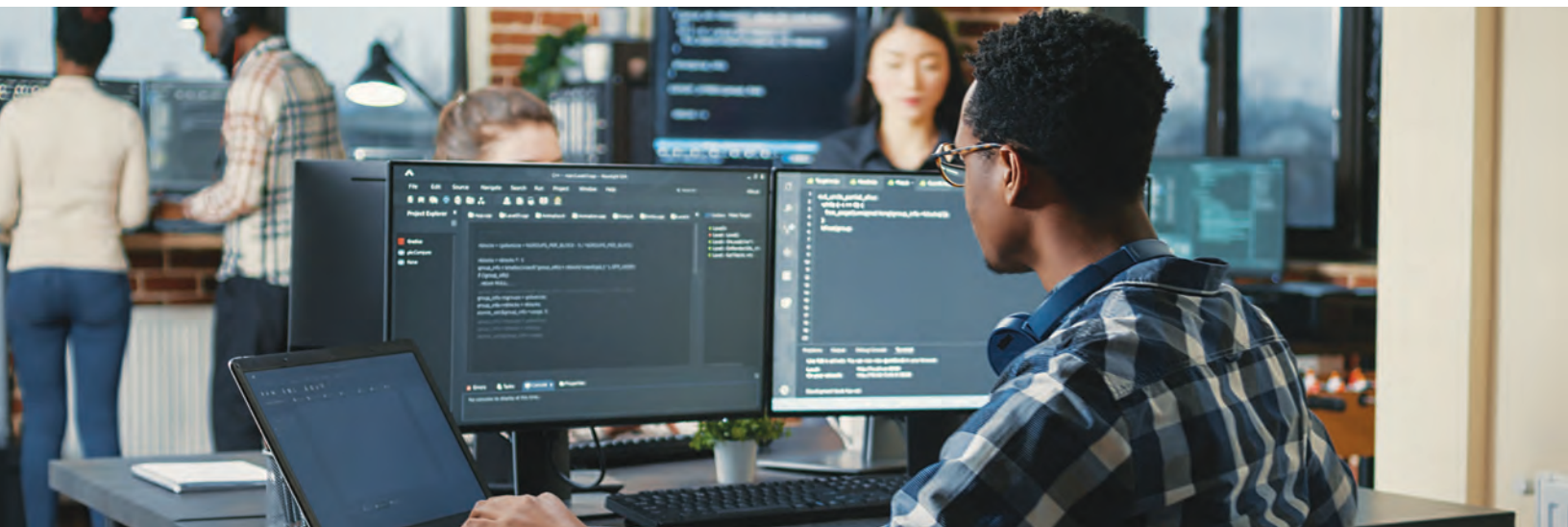
This illustrates a broader shift in the cyber threat environment: **the barrier to mounting a sophisticated attack on critical infrastructure is falling**, while the potential consequences, such as the cascading failures across energy, telecommunications, transportation and financial systems remain severe.

State-sponsored cyber attacks

The cyberthreat landscape includes state-sponsored attacks, with nation-states leveraging their hacking capabilities to target the essential systems of other countries to exert political influence, gather intelligence and disrupt operations.

During the first half of 2025, there were 3,018 cyber attacks predominantly targeting critical infrastructure, including the energy sector and government institutions.¹² Analysis of malware attacks revealed evidence of AI-assisted code generation. This reflects the fact that **AI's role in cyber attacks is no longer limited to phishing**, creating a real-time laboratory for understanding hybrid warfare.

Recent conflict across the Middle East has also seen critical infrastructures being targeted, including **state-sponsored cyber attacks on official news sites and security communications** systems, leading to near-total internet blackout. Hactivist groups targeted multiple government-aligned news websites by initiating denial-of-service (DoS) attacks.¹³



The silent infiltration inside US infrastructure networks

Moving beyond traditional data theft, state-sponsored threats are now focused on **infiltrating the critical infrastructure** of water, energy and telecommunications in the US.

In July 2025, threat actors compromised more than 400 US organizations through cloud-based platforms, including the Department of Energy, the Department of Homeland Security and the Department of Health and Human Services.

In the United States, a significant portion of critical infrastructure is owned and operated by the private sector, making public-private collaboration central to national resilience. In 2024, approximately **70% of all recorded cyber attacks successfully compromised infrastructure within the private sector.**¹⁴

Furthermore, state-affiliated actors maintained undetected access inside the network of a public power utility in Littleton, Massachusetts, for several months before the intrusion was detected.

The case illustrates a defining feature of such attacks known as **“pre-positioning,”** which is not designed for immediate impact, but for leverage. It ensures that, in the event of geopolitical escalation, adversaries already have a foothold in the systems that civilian populations depend on most.



Data centers at risk

With the growth in AI capabilities, **hackers are increasingly targeting data centers.** Bad actors can subvert AI models by gaining access to their weights, which govern model training and output.¹⁵

With **over USD500 billion going into data center construction in 2026,**¹⁶ businesses and societies are increasingly reliant on this infrastructure which is the backbone of digital transformation. At the same time, controversy surrounding the energy and water needs of such projects — particularly in developing countries — could expose data centers to social unrest and sabotage from disgruntled communities.

Moreover, **modern warfare is increasingly targeting data centers** to cause widespread service disruptions. A significant example includes the 2026 Middle East conflict, where data centers belonging to major cloud providers suffered extensive damage amid intensified military action.¹⁷

The attacks reportedly caused structural damage, disrupted power supply to critical infrastructure, and, in some cases, required fire suppression efforts, leading to further depletion of water supplies.

Ransomware continues to dominate

In its Global Cybersecurity Outlook 2026, the World Economic Forum found that Chief Information Security Officers (CISOs) ranked ransomware attacks as the greatest risk.¹⁸

Following the 2021 Colonial Pipeline ransomware attack, the US government had to declare a state of emergency, as the suspension of operations in the pipeline disrupted fuel deliveries to airports, panic-buying emptied forecourts across multiple states and national gas prices spiked.

Nearly two years after the attack, the Cybersecurity and Infrastructure Security Agency (CISA), focusing on **improving resilience of the Nation’s critical infrastructure,** reported on its development of a central location for alerts and guidance for businesses and individuals. It also launched the Joint Ransomware Task Force to form cohesive collaboration across the US government and established a community of experts on the front lines of cyber defense.

“For corporate risk managers, the Colonial Pipeline ransomware attack is an important one because it’s all about organizational resilience. It absolutely needs to be on the risk register and embedded into an overall enterprise and infrastructure risk management program. On a broader level, regulation around the protection of critical infrastructure is going to start to become a lot more onerous.”

— **John Farley**, Managing Director, Cyber Liability practice at Gallagher

Many of the entities responsible for overseeing critical infrastructure have adopted a gradual approach to embracing enhanced secure frameworks. The predicament is further complicated by the challenges in conveying the risks associated with operational technology and IT to board members and top-level executives.

Identifying high-value or “critical” assets and creating a comprehensive business continuity plan for their prioritized restoration in the event of cyber attacks is crucial.

Additionally, it’s essential to establish emergency communication channels between IT, operations and top executives to react swiftly and effectively to any cybersecurity compromises. A gap in communication can obstruct well-informed decision-making, further delaying the prompt execution of vital cybersecurity protocols.



4. Aging infrastructure

Risks are evolving as infrastructure is challenged to meet today's resource demands. At a time when rising debt costs are limiting governments' abilities to fund large-scale projects, the financial demands on infrastructure are only growing. Aging systems will require not just ongoing maintenance, but in some cases complete replacement, particularly where outdated technology can no longer be integrated with modern digital infrastructure.

Aging systems also require adequate critical infrastructure protection, including frequent maintenance and monitoring, as deteriorating structures will inevitably reach a point of failure, potentially resulting in severe injuries, loss of life and property damage. This ultimately brings critical infrastructure operations to a halt.

“The problem of aging infrastructure is more pronounced in the West. We’re seeing companies move from China to Mexico because supply chains are diverging from a geopolitical point of view. But then, when they get to Mexico, there’s not enough electricity for them to operate because the grids are aging and there hasn’t been enough investment.”

— **Adam Carrier**, Head of Consulting at AnotherDay,
A Gallagher Company

The scope of such events can be global, with knock-on implications for the supply chain, transport and health. Lack of investment in physical infrastructure in the current economic climate is a substantial threat, hampering economic progress and recovery, and exposing businesses and communities to significant risks.

The fact that public installations are often financed through taxes complicates matters further, with political preferences playing a crucial role in the timely release of funds. As a result, maintenance can often take a backseat to projects that have more public appeal.

Calgary’s catastrophic main break and the cost of deferred maintenance

On December 30, 2025, the Bearspaw South Feeder Main, a single pipe that supplies around 60% of treated water to Calgary’s 1.6 million residents, ruptured for the second time in 18 months.

After the feeder main broke, the city lost about 80 million liters of water and the reserve dropped to 459 million liters.¹⁹ This forced Calgary to rely almost entirely on its smaller secondary treatment facility to serve the entire city.

An independent review panel commissioned after the first break in June 2024 found the failures were tied to aging infrastructure and systemic issues in governance, asset integrity and risk management. Calgary’s mayor described the feeder main as having reached end-of-life, warning that no amount of patchwork repairs could restore it to reliable service.

The incident carries a lesson that extends far beyond Calgary. Infrastructure experts have warned it was a wake-up call for every city in Canada, where the true cost of aging water systems is increasingly being paid not in planned investment, but in emergency responses.



Securing essential systems and building critical infrastructure resilience

Future economic stability depends on something most people never think about until it fails, the essential systems that deliver power, water and connectivity every hour of every day. As the threats to these systems multiply — from cyber attacks and extreme weather to aging assets and geopolitical instability — critical infrastructure protection has moved from a policy ambition to an operational imperative.

Organizations that treat infrastructure resilience as a strategic priority, rather than a compliance exercise, will be better placed to minimize disruption when essential systems are put under pressure. That means rigorous scenario planning, robust business continuity frameworks and insurance programs stress-tested against the specific risks that critical infrastructure faces, not just in normal operating conditions, but also when those conditions break down.

Closing the gap between today's infrastructure vulnerabilities and tomorrow's demands requires more than individual action. It calls for deep collaboration between public and private sectors, sustained investment in both new and legacy physical infrastructure and a regulatory environment that actively incentivizes critical infrastructure protection. Policymakers must move beyond aspiration: joint planning, knowledge sharing and clear standards are the building blocks of genuine infrastructure resilience.

As digitalization reshapes essential systems and smart technologies are layered onto decades-old foundations, resilience must be designed in from the start rather than retrofitted after failure. The risks are too interconnected, and the consequences too far-reaching; it's essential to factor in the need for resilience in an increasingly uncertain and interconnected world.

“The definition of critical infrastructure is presently undergoing expansion. Satellite imagery collection, manufacture and design of semiconductors, and artificial intelligence also now fall within this category. With the broadening scope of critical infrastructure, regulatory frameworks are expected to continue evolving. This evolution is likely to encompass multiple areas.”

— **Adam Carrier**, Head of Consulting at AnotherDay, A Gallagher Company



Citations

¹[The Global Risks Report 2026](#)," *World Economic Forum*, accessed 8 Jan 2026. PDF file.

²[Government Progress Fixing Crumbling Schools and Hospitals](#)," *GOV.UK*, 10 Sep 2025.

³[Gartner Predicts That by 2028 Misconfigured AI Will Shut Down National Critical Infrastructure in a G20 Country](#)," *Gartner*, 12 Feb 2026.

⁴Thomas, Daniel, et al. "[Oil and Gas Prices Jump as Conflict Escalates](#)," *BBC*, 2 Mar 2026.

⁵Qiu, Winston. "[Finland Charges Russian-Linked Ship Officers Over Baltic Sea Cable Sabotage](#)," *Submarine Cable Networks*, 13 Aug 2025.

⁶Leicester, John, and Emma Burrows. "[At Least 11 Baltic Cables Have Been Damaged in 15 Months, Prompting NATO to Up Its Guard](#)," *AP News*, 28 Jan 2025.

⁷Igini, Martina. "[2025 One of Costliest Years for Climate Disasters: Report](#)," *Earth.Org*, 27 Dec 2025.

⁸[What Happened During the Biggest Geomagnetic Storm in Over 20 Years](#)," *NASA Scientific Visualization Studio*, 9 May 2025.

⁹Wallner, A.V.L., et al. "[The Geomagnetic Storm on 10-12 May 2024 and Its Effect on the Swedish Power Grid](#)," *Wiley: Space Weather*, Feb 2026.

¹⁰[2024 Super Typhoon Yagi](#)," *Center for Disaster Philanthropy*, 26 Nov 2024.

¹¹Bagwe, Mihir. "[UAE Blocked AI-Powered Terrorist Cyberattacks Targeting Critical Infrastructure](#)," *The Cyber Express*, 23 Feb 2026.

¹²Lakshmanan, Ravie. "[From Phishing to Malware: AI Becomes Russia's New Cyber Weapon in War on Ukraine](#)," *The Hacker News*, 9 Oct 2025.

¹³Butts, Dylan. "[The Digital Front: Iran's Internet Blackout Enters Fourth Day Amid Reports of Cyberattacks](#)," *CNBC*, 3 Mar 2026.

¹⁴[Threat Snapshot: Cyber Threats Remain Heightened Amid Lapse in Information Sharing Authorities, Government Shutdown](#)," *Homeland Security Republicans*, 31 Oct 2025.

¹⁵Stansbury, Martin, et al. "[Can US Infrastructure Keep Up With the AI Economy?](#)" *Deloitte*, 24 Jun 2025.

¹⁶Sigalos, MacKenzie. "[OpenAI's First Data Center in \\$500 Billion Stargate Project Is Open in Texas, With Sites Coming in New Mexico and Ohio](#)," *CNBC*, 24 Sep 2025.

¹⁷Vincent, Brandi. "[Commercial Data Centers Emerge as Targets in Modern Warfare After Drones Hit 3 AWS Facilities](#)," *DefenseScoop*, 3 Mar 2026.

¹⁸[The Cyber Threats to Watch in 2026 – and Other Cybersecurity News](#)," *World Economic Forum*, 19 Feb 2026.

¹⁹Krause, Darren. "[Two-Week Timeline Targeted for Bears paw Feeder Main Repairs](#)," *Livewire Calgary*, 1 Jan 2026.

Keep up to date with the latest news
and insights visit **[AJG.com/insights](https://www.ajg.com/insights)**

CONDITIONS AND LIMITATIONS

This information is not intended to constitute any form of opinion nor specific guidance nor legal or financial advice, and recipients should not infer such from it or its content. Recipients should not rely exclusively on the information contained in the bulletin and should make decisions based on a full consideration of all available information. We make no warranties, express or implied, as to the accuracy, reliability or correctness of the information provided. Our advice to our clients is provided subject to specific terms and conditions, the terms of which take precedence over any representations in this document. We and our officers, employees or agents shall not be responsible for any loss whatsoever arising from the recipient's reliance upon any information we provide and exclude liability for the statistical content to fullest extent permitted by law.