Report: America’s Critical Infrastructure is Highly Vulnerable
Fending Off Cyber Threats—and Building Resiliency—Will Require Deeper Public-Private Collaboration


The report comes at a time when the United States is facing unprecedented challenges in safeguarding its critical infrastructure from both disruption and direct attack. Several factors are fueling heightened concern about the resiliency of these vital systems: escalating geopolitical tensions, the rapid integration of network-connected and automated technologies, systems that are growing more antiquated—and vulnerable—by the day; and the fact that the private sector operates most of the nation’s critical infrastructure.

The Solutions Brief can be found here and is the latest in CED’s Sustaining Capitalism series. It details the challenges of—and provides recommendations for—securing US critical infrastructure and building resiliency, focusing on three vital areas as case studies: water systems, energy, and communications.

“As cyberattacks escalate in number and complexity, it is crucial to build critical infrastructure systems that are robust and resilient. The overriding solution is deeper collaboration between public and private sector leaders. Key components of the partnership include building in resiliency to shorten if not eliminate the turnaround time to get systems back up, and training a second-to-none cybersecurity workforce that is both large and sophisticated enough to keep our systems secure—no easy feat, but paramount in an era where the only certainty is constant attacks that continuously evolve,” said Dr. Lori Esposito Murray, President of CED.

By the Numbers: Cyberattacks and Threats

- **94 percent**: The share of businesses with 100+ employees that experienced a cyberattack in 2022.
- **$8 trillion**: The expected global cost of cybercrime in 2023.
- **81 percent**: The increase in cyber threats that organizations experienced at the start of the pandemic.
- **100 percent**: From 2021 to 2022, the share of cyberattacks led by nation-states targeting critical infrastructure grew by 100 percent (going from 20 to 40 percent). This is largely due to Russia’s goal of damaging Ukrainian infrastructure, and espionage targeting Ukraine’s allies, including the US.
• **$1.9 trillion:** A hypothetical catastrophic cyberattack on energy plants that leaves nearly 100 million people without power for weeks would cost the US economy up to $1.9 trillion over six years.

Key Recommendations from the Solutions Brief:
1) Increase collaboration and information-sharing between government and the private sector, prioritizing operators of critical infrastructure.
   - Clearly define and strengthen the role of the Cybersecurity and Infrastructure Security Agency (CISA) as national coordinator to lead the national cybersecurity efforts.
   - The Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) should be expeditiously implemented by CISA and Sector Risk Management Agencies (SRMAs).
   - Harmonize and deconflict reporting requirements as new CIRCIA, Securities and Exchange Commission (SEC), and sector-specific frameworks are implemented.
   - Update the 2013 presidential directive governing critical infrastructure efforts across federal agencies.
   - Provide guidance to SRMAs on updating sector plans and minimizing the amount of remediation time to strengthen resiliency.
   - Promote participation of critical infrastructure firms in CISA’s Sector Coordinating Councils (SCCs).
   - Critical infrastructure owners and operators must make cybersecurity a top governance priority, which should include a review of supply chains for vulnerabilities.

2) Strengthen the resiliency of critical infrastructure and the government’s ability to detect and respond to cyberattacks and threats.
   - Fund implementation of the National Cybersecurity Strategy, utilizing available funding from the Bipartisan Infrastructure Bill and the Inflation Reduction Act.
   - Raise awareness of and expand the provision of federal resources and technical assistance.
   - Require that CISA define systemically important entities.
   - Encourage the private sector to adopt robust security measures, including working jointly with government leaders to pursue the development of minimum standards for critical sectors.
   - Assess applications for artificial intelligence (AI) in critical systems and threats of AI use in cyber warfare.
   - Invest in building a cybersecurity workforce with skills to secure critical systems.
Media Contact
adonovan@tcb.org

About CED
The Committee for Economic Development (CED) is the public policy center of The Conference Board. The nonprofit, nonpartisan, business-led organization delivers well-researched analysis and reasoned solutions in the nation’s interest. CED Trustees are chief executive officers and key executives of leading US companies who bring their unique experience to address today’s pressing policy issues. Collectively they represent 30+ industries, over a trillion dollars in revenue, and over 4 million employees. www.ced.org

About The Conference Board
The Conference Board is the member-driven think tank that delivers trusted insights for what’s ahead. Founded in 1916, we are a non-partisan, not-for-profit entity holding 501 (c) (3) tax-exempt status in the United States. www.ConferenceBoard.org