Homeland Security

7

Real estate is a critical part of the nation's infrastructure. The industry faces an array of threats from natural catastrophes, international and domestic terrorism, criminal activity, cyber-attacks, and more. The Roundtable prioritizes strengthening the security and resilience of the commercial facilities sector as it is essential to safeguarding any facility where people live, work, shop, and play.

HSTF and RE-ISAC

Through increased cross-agency information sharing and cooperation with key law enforcement and intelligence agencies, The Roundtable's Homeland Security Task Force (HSTF) and Real Estate Information Sharing and Analysis Center (RE-ISAC) remain focused on measures that businesses can take to address these issues, including risk mitigation measures that increase resilience and resistance to physical damage and cyber breaches. Through these bodies, The Roundtable acts as a convener between public and private sector entities to address some of the most pressing security issues facing our country.

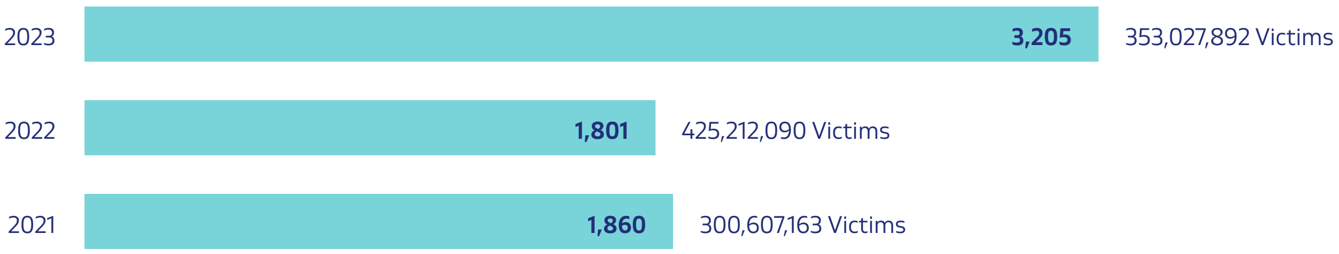
Among the HSTF's activity this year, the group held a meeting at The Roundtable's 2024 State of the Industry meeting to address Chinese espionage efforts impacting American corporations, the emerging use of Artificial Intelligence as a new risk vector, and the current dynamic in pricing and coverage in commercial insurance markets.

HSTF and RE-ISAC meet regularly and continue to work closely with federal, state, and local officials on potential cyber and physical threats to our industry, organized criminal activity, and against the misuse of commercial real estate assets in the subversion of domestic or international law.

Cyber and Physical Threats

Growing geopolitical conflicts have raised security concerns about cyberattacks and exposed existing vulnerabilities in the nation's cybersecurity regime, heightening the necessity to build robust domestic defense systems.

Total Compromises, Year over Year



Between 2021 and 2023 data breaches in the U.S. rose 72%.[21]

For the 13th consecutive year, the United States held the title for the highest data breach costs. The top five countries or regions with the highest average cost of a data breach saw considerable changes from 2022.

$9.44 M

United States 2022

$9.48 M

United States 2023

The average cost of a data breach for a company in the U.S. is $9.48 million—the highest among other countries, and a 0.4% increase from 2022.[22]

The Roundtable and other national partners support the passage of bipartisan legislation that would advance America's public and private efforts to safeguard cyberspace and enhance the nation's economic competitiveness in a global digital economy.

Roundtable comments were also cited nearly a dozen times in a final SEC rule requiring public companies to disclose more information about cybersecurity-related incidents, risk management, strategy, and governance. The Roundtable is working through a coalition of business organizations to ensure that any cyber incident reporting legislation creates a compliance regime that treats cyber-attack victims as victims, provides affected businesses with clarity in reporting, encourages cooperation between the public and private sectors, and limits legal liability.

Planning for Significant Events

As part of the *2021 National Defense Authorization Act (NDAA)*, Congress mandated that the president develop a Continuity of the Economy Plan (COTE) to maintain and restore the economy in response to a significant event. Among other things, the plan requires an analysis of U.S. distribution and supply chains to identify the critical economic actors and functions that must be operational if the U.S. is to maintain its defense readiness, public health, and national security.

The Roundtable's focus is specifically on the Commercial Facilities (CF) Sector and the potential impacts on real estate from a wide-scale event. Given the crucial role the sector plays in facilitating interaction and communication with critical infrastructure owners, operators, and relevant stakeholders, The Roundtable has included key partners in our discussions with the COTE Project Team to provide insights and input on the COTE scoping effort from our community.

The Roundtable will continue aiding efforts by CISA's National Risk Management Center to develop the COTE plan.

As the Ranking Member on the Senate Armed Services Committee's Subcommittee on Cybersecurity Sen. Mike Rounds (R-SD) discusses the need to enhance our nation's cyber capabilities.