Homeland Security

As a critical part of the nation's infrastructure, real estate continues to face an array of threats from natural catastrophes, international and domestic terrorism, criminal activity, cyber-attacks, and border security. To address such threats, The Roundtable continues to help build a more secure and resilient industry against both physical and cyber threats.

The Real Estate Information Sharing and Analysis Center (RE-ISAC)

The RE-ISAC is a public-private partnership between the U.S. commercial facilities sector and federal homeland security officials organized by The Roundtable in February 2003. Information sharing in a systematic and sustained manner continues to be one of the most effective weapons in protecting the nation's critical infrastructure. The RE-ISAC serves as the primary conduit of terrorism, cyber- and natural-hazard warning and response information between the government and the commercial facilities sector. The RE-ISAC proactively manages risk and strengthens the security and resilience of the U.S. commercial facilities sector infrastructure to aid protection and prevention.

Homeland Security Task Force (HSTF)

The Roundtable works with various federal, state, and local law enforcement agencies through its HSTF. The HSTF identifies, analyzes, and advocates for positions on physical and cyber security policy affecting the real estate community and commercial facilities sector in relevant homeland security and intelligence issue areas. In addition to working with relevant law enforcement and intelligence agencies, the HSTF is working to find new sources and methods to secure high-profile commercial-facility-sector assets and improve their emergency preparedness. Through the work of the HSTF and RE-ISAC, real estate firms are regularly updated on cyber, criminal, and physical threats and how to appropriately implement security measures to help mitigate risks.

As a member of the Senate Foreign Relations, Homeland Security & Government Affairs Committees Sen. Mitt Romney (R-UT) discussed the committees' work on addressing ransomware attacks, cyber security, and international and domestic terrorism.

Improving Resilience to Cyber and Physical Threats

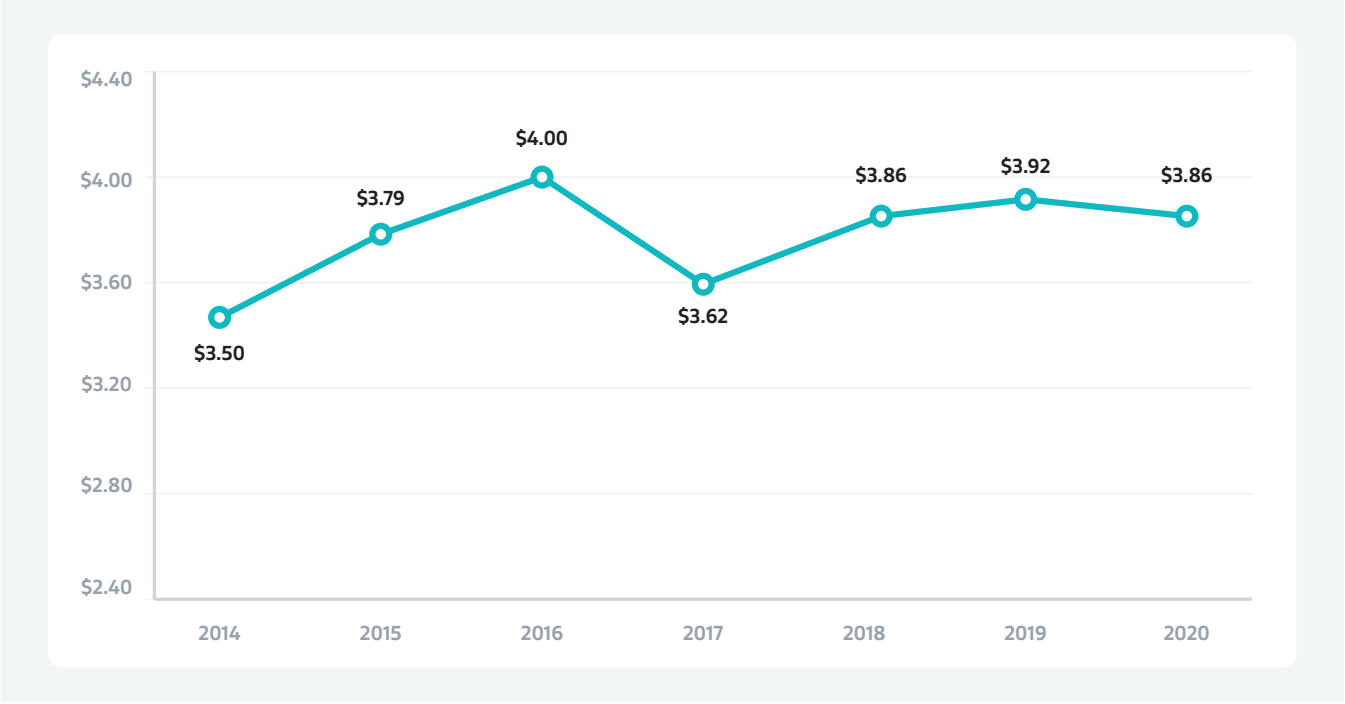
Through the HSTF and RE-ISAC, The Roundtable remains focused on measures that businesses can take through increased cross-agency information sharing and cooperation with key law enforcement and intelligence agencies — such as creating resilient infrastructure that is resistant to physical damage and cyber breaches. Bipartisan legislation that would require private companies to report ransomware attacks to federal authorities was advanced by the Senate Homeland Security and Governmental Affairs Committee in October 2021. The proposed legislation would require certain critical infrastructure owners and operators to report cyber-attacks within 72 hours and

ransom payments within 24 hours to the Cybersecurity and Infrastructure Security Agency (CISA).

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. The Roundtable recommends policymakers include several provisions as part of a mandatory reporting regime, including:

- Establish a prompt reporting timeline of not less than 72 hours. Legislation should reflect an appropriate, flexible standard for notifying the government about significant cyber incidents.
- Attach reporting to confirmed cyber incidents. Businesses need clarity in reporting requirements, which should be targeted to well-defined and confirmed cyber incidents.
- Confine reports to significant and relevant incidents. A list should be limited in reach—particularly excluding small businesses using existing federal rules—and risk based.
- The business industry comments recommended that federal cybersecurity reporting legislation should also include robust liability protections; consistent federal reporting requirements; restrictive government use of reported data; and guarantee substantial input from industry to protect the rulemaking process.

Average total cost of a data breach
Measured in US $ millions



Source: IBM Security, July 2021.