The Real Estate Roundtable

Cyber and Physical Threats to U.S. Real Estate

Homeland Security

Summary

The rising incidence of violent crime, organized retail crime, civil unrest, cyber-attacks, artificial intelligence (AI), and the renewed threat of terrorism have prompted increased vigilance, information sharing, and legislative efforts to improve our nation's resilience. The proliferation of these threats has raised concerns in the commercial facilities sector about how to protect commercial properties and the people who occupy them from such threats.

In addition to the challenges posed by these threats, the Russian invasion of Ukraine, conflict in the Middle East, and rising tensions in Asia have raised security concerns about the increased incidence of cyber-attacks from the Russian Federation, the People's Republic of China (PRC), Iran, North Korea, and other state actors.

Information sharing is vital for the commercial facilities sector to enhance cybersecurity, improve incident response, mitigate physical threats, build community resilience, and maintain a competitive edge by fostering collaboration and innovation among different facilities and organizations.

The real estate industry, in partnership with policymakers and law enforcement officials, must remain vigilant to potential threats to our critical infrastructure from cyber or physical threats.

Key Takeaways

- Recent high-profile hacking attacks have brought to the fore the necessity of **fortifying the nation's IT infrastructure against cyber-attacks**. Additionally, there are **growing concerns about AI having the potential to create new risks**. Key concerns include the risk of cyberattacks exploiting AI vulnerabilities, leading to unauthorized access to facilities or sensitive data.
- RER continues to promote security measures against both physical and cyber threats by facilitating increased information sharing and cooperation among its membership with key law enforcement and intelligence agencies, including as part of RER's **Homeland Security Task Force and Real Estate Information Sharing and Analysis Center (RE-ISAC)**.
- Policymakers should avoid imposing duplicative and inconsistent regulations that create additional challenges for those tasked with defending the nation's critical infrastructure, including the commercial facilities (CF) sector, and undermine cyber preparedness.

Background

CISA 2015 Reauthorization – Critical for Information Sharing

- The Cybersecurity Information Sharing Act of 2015 (CISA 2015) was designed to encourage and protect the sharing of cyber threat information between private sector companies and the federal government. The act was a cornerstone of public-private partnership in cybersecurity, enhancing national defense and economic security. Yet, Congress failed to reauthorize CISA 2015, and it expired on September 30, 2025 amid the government shutdown fight.
- The primary impact of this lapse is the loss of specific legal protections for private companies sharing cybersecurity threat information with the government. While sharing may continue, the lack of explicit liability and antitrust shields could reduce the flow of critical threat intelligence, weakening a key defense against increasingly sophisticated cyberattacks.
- The House Homeland Security Committee, led by Chairman Andrew Garbarino (R-NY), advanced a reauthorization bill, the *Widespread Information Management for the Welfare of Infrastructure and Government (WIMWIG) Act* (H.R.5079). Chairman Garbarino's bill seeks to reauthorize CISA 2015 for 10 years and update it to address artificial intelligence and supply chain threats.
- Reauthorization efforts stalled in the Senate, primarily due to objections from Senator Rand Paul (R-KY). Sen. Paul blocked efforts to pass a clean reauthorization, citing concerns about CISA's involvement in combating online misinformation and disinformation. The Real Estate Roundtable supports Chairman Garbarino's bill and is working to advance this important legislation.

National Cybersecurity Strategy

- First released in early 2023, the U.S. National Cybersecurity Strategy was designed to "secure the full benefits of a safe and secure digital ecosystem for all Americans" and bolster collaboration between the public and private sectors to ensure a secure cyber ecosystem, according to a White House statement.
- In May 2024, the U.S. government announced that several aspects of the U.S. National Cybersecurity Strategy were advanced or had gone into force. This includes progress on scores of objectives, including developing cybersecurity scenario exercises to help critical infrastructure owners prepare for attacks from nation states and malicious cyber actors and proposing changes to the way the government maintains security.
- The strategy also aims to ensure that the U.S. stays at the forefront of developing cybersecurity standards and establishes a State Department Bureau of Cyberspace and Digital Policy to build international partnerships to counter malicious cyber actors.
- The Office of the National Cyber Director (ONCD) issued a report that discusses its efforts to develop "a comprehensive policy framework for regulatory harmonization" that aims to "strengthen" cybersecurity resilience across critical infrastructure sectors, "simplify" the work of sector-specific regulators while taking advantage of their unique expertise, and "substantially reduce the administrative burden and cost on regulated entities." Comments indicate frustration with a disjointed regulatory environment that increased compliance costs without a commensurate enhancement in cybersecurity.
- The ONCD plans to use the report to inform its pilot effort to develop a reciprocity framework for a designated critical infrastructure sector. A companion blog post from the head of ONCD describes the pilot as seeking to "design a cybersecurity regulatory approach from the ground up." The blog calls on Congress for help to bring relevant agencies together "to develop a cross-sector framework for harmonization and reciprocity for baseline cybersecurity requirements."

Recommendations

Strengthen Preparedness and Info Sharing: Policymakers and law enforcement agencies must advance efforts to counter potential physical and cyber threats, especially to critical infrastructure. The real estate industry remains an important partner in these efforts.

- As a critical part of the nation's infrastructure, real estate continues to assess and strengthen its cyber and physical defenses to protect our industry from an array of threats.
- In addition to civil unrest, organized retail crime, and violent attacks on properties across the U.S., real estate continues to face a variety of cyber and physical threats, such as:
    - Disruptive and destructive cyber operations against strategic targets, including an increased interest in control systems and operational technology;
    - Cyber-enabled espionage and intellectual property theft;
    - Improvised explosive devices (IEDs);
    - Attacks against U.S. citizens and interests abroad and similar attacks in the homeland;
    - Tenant fraud; and
    - Unmanned aircraft system (UAS) attacks against hardened and soft targets.
- Through a Cybersecurity Information Sharing and Collaboration Agreement with DHS's CISA, the RE-ISAC engages in operational efforts to better coordinate activities supporting the detection, prevention, and mitigation of cybersecurity, communications reliability, and related data threats to critical infrastructure.
- RER supports the *WIMWIG Act* (H.R.5079) introduced to reauthorize CISA 2015 for 10 years and update it to address artificial intelligence and supply chain threats.
- RER remains focused on measures that businesses can take—such as creating resilient infrastructure that is resistant to physical damage and cyber breaches—to better prepare for potential threats.