The Real Estate Roundtable

Cyber and Physical Threats to U.S. Real Estate

Homeland Security

Summary

Rising incidence of cyber and physical security threats—including terrorism, cyberattacks, and organized crime—have heightened concerns about protecting commercial properties and critical infrastructure.

The conflict in Iran raises additional security concerns. Iran poses a credible, near-term threat to the U.S. homeland, utilizing cyber operations, targeted assassination plots against officials, and potential proxy network activations to retaliate against U.S. strikes in the Middle East. Increased risks include cyberattacks on critical infrastructure, violent extremist radicalization, and attacks on religious or government targets by Iran-linked actors.

The Islamic Revolutionary Guard Corps (IRGC) and its affiliates are capable of conducting asymmetric operations and creating and strengthening proxy networks within the U.S. The conflict has prompted warnings from the FBI regarding intelligence, espionage, and potential attacks from Iran-linked individuals.

The conflict may motivate homegrown violent extremists or Iranian proxies to launch attacks on U.S. soil, targeting public gatherings, faith-based institutions (synagogues, mosques), and universities. While direct state-sponsored attacks are less common, Iran may leverage its global network of proxies, such as Lebanese Hezbollah, or activate "sleeper cells" to carry out asymmetric retaliation.

In addition to the challenges posed by Iran and its proxy groups, the ongoing Russian invasion of Ukraine 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), 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.

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 supports enhanced information sharing and cooperation among its membership with key law enforcement and intelligence agencies through its **Homeland Security Task Force and Real Estate Information Sharing and Analysis Center (RE-ISAC)**.
- Policymakers should avoid imposing duplicative or inconsistent regulations that create additional challenges for those tasked with defending the nation's critical infrastructure 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. CISA 2015 is currently active following a short-term extension that expires on Sept. 30, 2026. The law, which provides liability and privacy protections for companies sharing cyber threat data with the government, originally featured a 10-year sunset clause that led to several lapses and temporary renewals starting in late 2025.
- This law is important for our sector as it provides 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), continues to advance 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.
- RER 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.

- 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* introduced to reauthorize and make updates to CISA 2015.
- 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.