Homeland Security

Cyber and Physical Threats

Issue

The rising incidence of violent crime, organized retail crime, civil unrest, cyber-attacks, 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 and the reduction of funding for many state and local law enforcement agencies have 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 remaining challenges posed by the pandemic, the Russian invasion of Ukraine has raised security concerns about the increased incidence of cyber-attacks from the Russian Federation and other state actors.

Talking Points

- Recent high-profile hacking attacks have brought to the fore the necessity of fortifying the nation's IT infrastructure against cyber-attacks.
- On March 15, 2022, President Biden signed into law the Cyber Incident Reporting for Critical Infrastructure Act, which was included in an omnibus appropriations bill. Against the backdrop of high-profile cyber-attacks on critical infrastructure providers and growing concerns of retaliatory cyber-attacks relating to Russia's invasion of Ukraine, the House approved the bipartisan legislation on March 9 and the Senate unanimously approved the legislation on March 11.
- The Act creates two new reporting obligations on owners and operators of critical infrastructure:
    - An obligation to report certain cyber incidents to the Cybersecurity and Infrastructure Security Agency (CISA) of the U.S. Department of Homeland Security (DHS) within 72 hours, and
    - An obligation to report ransomware payments within 24 hours.
- The new reporting obligations will not take effect until the Director of CISA promulgates implementing regulations, including "clear description[s] of the types of entities that constitute covered entities."
- In addition, the SEC has proposed regulations that would require public companies to make prescribed cybersecurity disclosures. The proposed rules would "strengthen investors' ability to evaluate public companies' cybersecurity practices and incident reporting" by requiring:

Cyber and Physical Threats

Talking Points (Continued)

  - (i) mandatory, material cybersecurity incident reporting, including updates about previously reported incidents; and
  - (ii) mandatory, ongoing disclosures on companies' governance, risk management, and strategy with respect to cybersecurity risks, including board cybersecurity expertise and board oversight of cybersecurity risks.

- The Roundtable submitted comments on the proposed SEC rules for submission on May 9, 2022. In the letter, we cite our long history of support for effective information sharing and policies that promote industry reporting to the federal government on significant cybersecurity incidents. We also raise a number of concerns regarding the detailed, granular reporting that would be required by the Proposal, and the rigid incident reporting deadlines, which members fear may unintentionally exacerbate cybersecurity risks for issuers and impose burdens unjustified by obvious benefits.
- 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.
- Through our Homeland Security Task Force and Real Estate Information Sharing and Analysis Center (RE-ISAC), The Roundtable remains focused on measures that businesses can take—such as creating resilient infrastructure that is resistant to physical damage and cyber breaches—through increased cross-agency information sharing and cooperation with key law enforcement and intelligence agencies.
- Through a Cybersecurity Information Sharing and Collaboration Agreement with DHS's Cybersecurity and Infrastructure Security Agency (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.

Cyber and Physical Threats

Talking Points (Continued)

- 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;
    - pandemic risk; and
    - unmanned aircraft system (UAS) attacks against hardened and soft targets.
- 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—international and domestic terrorism, criminal activity, cyber-attacks, border security, and natural catastrophes.
- The Roundtable 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.

Homeland Security

Cyber and Physical Threats: Continuity of the Economy Plan (COTE)

Issue

Pursuant to Section 9603 of the 2021 National Defense Authorization Act (NDAA), Congress mandated that the President shall develop and maintain a Continuity of the Economy Plan (COTE) to maintain and restore the economy of the United States in response to a significant event. Despite having Continuity of Operations (COOP) and Continuity of Government (COG) plans to ensure the nation could function after a nuclear attack, no equivalent effort exists to ensure the rapid restart and recovery of the U.S. economy after a catastrophic or major disruption. Such disruptions could include a large-scale cyberattack or any other severe degradation that compromises the national conveyance of goods or services. Following such a catastrophic event, the government will have to prioritize its limited recovery resources, governed by a COTE Plan. A COTE will provide the U.S. with a robust and adaptable framework to restore the economy after a catastrophic attack.

Talking Points

- The Roundtable has been working with the Cybersecurity and Infrastructure Security Agency's (CISA) National Risk Management Center to aid their efforts to develop a Continuity of the Economy Plan (COTE) to maintain and restore the U.S. economy in response to a significant event. CISA works with government and industry to identify, analyze, prioritize, and manage the most significant strategic risks to the nation's critical infrastructure.
- The Roundtable's focus is on the Commercial Facilities (CF) Sector and the potential impacts on real estate from a wide-scale 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.
- Given the crucial role that the CF Sector plays in facilitating interaction and communication with critical infrastructure owners, operators and relevant stakeholders, we are including key partners in our discussions with the COTE Project Team to provide insights and input on the COTE scoping effort from our community.