Cyber and Physical Threats

Issue

The rising incidence of cyberattacks, civil unrest and renewed threat of terrorism have prompted increased vigilance, information sharing and legislative efforts to improve our nation's resilience. The proliferation of civil unrest and the diminution of funding for state and local law enforcement agencies has raised concerns in the commercial facilities sector about how to protect businesses from such threats. In addition, the fall of Afghanistan has raised concerns about a revival of Al-Qaeda and their ability to project terrorist attacks on the homeland.

Talking Points

- The hack of IT management firm SolarWinds, which resulted in the compromise of hundreds of federal agencies and private companies, and the May 2021 ransomware attack on the Colonial Pipeline, as well as a recent onslaught of ransomware attacks affecting thousands of public and private entities have raised renewed concerns about enhancing the nation's cyber security.
- In July, U.S. Sen. Mark R. Warner (D-VA), Chairman of the Senate Select Committee on Intelligence, U.S. Sen. Marco Rubio (R-FL), Vice Chairman of the Committee, and U.S. Sen. Susan Collins (R-ME), a senior member of the Committee, introduced bipartisan legislation -- "Cyber Incident Notification Act of 2021 (S. 2047)" –that would require federal agencies, government contractors, and critical infrastructure owners and operators to report cyber intrusions within 24 hours of their discovery.
- The Roundtable is working through a coalition of business organizations to ensure that any cyber incident reporting legislation creates a compliance regime that treats cyberattack 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.
- In addition to civil unrest 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;

Cyber and Physical Threats

Talking Points (Continued)

  - » 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 help enhance resilience and security against both physical and cyber threats – focusing on measures that businesses can take to mitigate and manage risks from physical damage, cyber breaches and pandemic outbreaks – through increased cross-agency information sharing and cooperation with key law enforcement and intelligence agencies.