Cyber and Physical Threats

Issue

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 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 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, and other state actors.

The Roundtable's Position

- 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.
- On June 4, 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."

Cyber and Physical Threats

- On June 5, the Senate Homeland Security and Governmental Affairs Committee (HSGAC) held a hearing titled "Streamlining the Federal Cybersecurity Regulatory Process: The Path to Harmonization." Chairman Gary Peters (D-MN) announced he is working on legislation (a draft of which is attached) that would build on the pilot efforts initiated by the ONCD to harmonize the patchwork of information security and cybersecurity regulations applicable to regulated companies particularly the 16 critical infrastructure sectors.
- The Roundtable has raised concerns that duplicative and inconsistent regulations create additional challenges for those tasked with defending the nation's critical infrastructure, including the CF sector, and undermine cyber preparedness. Policymakers must work together to identify and address this overlap. We look forward to working with policymakers toward a more effective framework and welcome input from our members.
- On March 15, 2022, President Biden signed into law the Cyber Incident Reporting for Critical Infrastructure Act (CIRCA), 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."

Cyber and Physical Threats

- The CIRCIA Notice of Proposed Rulemaking (NRPM) was recently released, and the Roundtable plans to submit comments in conjunction with our colleagues on the Commercial Facilities Sector Coordinating Council to inform the direction and substance of the Final Rule.
- The NPRM contains proposed regulations for cyber incident and ransom payment reporting, as well as other aspects of the CIRCIA regulatory program. Implementation of CIRCIA will enable CISA to develop insights on the cyber threat landscape to drive cyber risk reduction across the nation and to provide early warning to entities who may be at risk of targeting. The comments CISA received through the Request for Information (RFI) and listening sessions over the past year helped shape this NPRM. In turn, getting robust input on the NPRM will support our ability to implement CIRCIA to drive national cyber risk reduction.
- In addition, the Securities and Exchange Commission (SEC) in July adopted rules requiring registrants to disclose material cybersecurity incidents they experience and to disclose on an annual basis material information regarding their cybersecurity risk management, strategy, and governance. The new rules require:
    - (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.

Homeland Security

Cyber and Physical Threats

- 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 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, 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.