October 2023

Cybersecurity Threats Trigger Industry-Wide Call to Action

Jonathan Todd & Megan MacCallum | BENESCH LAW

3PL Perspectives

ADOBE STOCK/BLUE PLANET STUDIO

CYBERSECURITY VULNERABILITY IS emerging as a top-of-mind issue for transportation and logistics service providers, regulators, and criminals alike. Recent years have yielded head line worthy ransomware attacks on domestic industry and critical infrastructure including malicious operations by foreign threat actors. The risk of public, costly, and potentially crippling incidents is on the rise, as is risk mitigation.

Examples of real or potential threats paint a stark picture. In May 2021, criminal

Examples of real or potential threats paint a stark picture. In May 2021, criminal hackers launched a ransomware cyberattack on American oil company Colonial Pipeline. The attack on this often-overlooked means of surface transportation resulted in a multi-million-dollar ransom payment in just hours. The impact included a reported six-day shutdown of the company's operating systems.

The federal government publicly ramped up directives around cybersecurity in an effort to raise industry awareness and instill best practices in subsequent years. In March of 2021, President Biden signed the Cyber Incident Reporting for Critical Infrastructure Act into law. The Act applies broadly to covered entities identified as critical to infrastructure across sectors. The Act requires that covered entities report certain cybersecurity incidents to the U.S. Cybersecurity and Infrastructure Security Agency ("CISA") within 72 hours and report ransomware payments to CISA within just 24 hours. In February 2022, Russia's invasion of Ukraine stepped up the urgency of cybersecurity matters and particularly their impact on the global supply chain. CISA issued a public warning regarding the risk of Russian cyberattacks against U.S. networks in retaliation for U.S. sanctions. By March, the White House issued intelligence-based warnings that Russia is considering engaging in cyberattacks against domestic U.S. interests. Private industry is viewed as critical to CISA's "Shields Up" strategy to prepare for and respond to cyberattacks.

Transportation and logistics as a sector may be particularly vulnerable to attack due to its essential character in all manner of industry and its voluminous interconnected relationships around the world (often with antiquated systems). Domestically, the Transportation Services Administration ("TSA") stands at the forefront of the cybersecurity issue for the transportation sector. Following the Colonial Pipeline attack in 2022, the TSA issued a Security Directive under its emergency authority. The Directive required pipeline owners and operators to: (1) report actual and potential cybersecurity incidents to CISA; (2) designate a Cybersecurity Coordinator to serve as a point person between a service provider and the TSA who is available 24 hours a day, seven days a week; (3) review current practices applicable to cybersecurity; and (4) identify vulnerability in cybersecurity and develop a plan to address cybersecurity risks and report the results to TSA and CISA. The TSA later updated its guidance to require additional measures including: (1) implementation of mitigation measures to protect against

ransomware and IT attacks; (2) implementation of a cybersecurity contingency and recovery plan; and (3) conducting a cybersecurity architecture design review.

The TSA's attention quickly spread to other modalities under its jurisdiction. The Administration issued similar directives for other segments including the railroad industry and for public transportation. The published Security Directives were designed to target higherrisk freight railroads, passenger rail, and public bus transportation. The operational framework largely mirrors the pipeline industry: (1) reporting cybersecurity incidents to CISA; (2) designation of a round-the-clock cybersecurity coordinator; (3) developing a cybersecurity incident response plan; and (4) developing a cybersecurity vulnerability assessment to identify gaps in security. The TSA has since continued its urgent cybersecurity initiatives. Most recently, in March 2023, it issued new cybersecurity amendments on an emergency basis to TSA-regulated airport and aircraft operators requiring updates to their security programs.

Other new federal programs outside the jurisdiction of transportation agencies have direct impact on the sector. The White House has introduced a Freight Logistics Optimization Works ("FLOW") initiative designed to promote the sharing of critical freight information between different supply chain participants. The digital infrastructure of FLOW is intended to strengthen supply chains by facilitating more frequent and more accurate information. The objective is to reduce COVIDtype disruptions and guard against interference through cybersecurity vulnerabilities and other threats. The initial participants in FLOW include the U.S. Department of Transportation and the Ports of Long Beach and Los Angeles, as well as the Georgia Ports Authority, terminal operators, private businesses and logistics and warehousing providers. Private participants are reported to include Nike Inc., Albertsons Companies., Target Corp., Walmart Inc., Union Pacific Corp., FedEx Corp., and Maersk.

Just as modern supply chains are global, these cyber concerns and mitigation efforts are not unique to the U.S. On Dec. 14, 2022, the European Parliament issued a Directive on measures for a high level of cybersecurity across the E.U. The Directive designated as "sectors of high criticality" key industry hubs and participants including airports, airlines, traffic control authorities, ports, port equipment operators, and shipping lines. Each of those identified will be required

under the Directive to put together an incident response team with resources and technical capabilities to handle cybersecurity threats real-time. The Directive also bolstered reporting requirements incumbent on companies that suffered a cybersecurity attack by requiring the European Union Agency for Cybersecurity ("ENISA") to develop rules for measuring and handling cybersecurity readiness and to develop a template for incident response.

The global effort against nefarious actors, and the well-being of private industry, requires vigilant day-to-day practices in order to be effective. Our industry has long concerned itself with operational best practices for achieving key metrics such as on-time delivery. It is now time to also give attention to building tech-savvy teams that can conduct nuanced vulnerability reviews to address the receipt of critical data, including personal information, and the personnel who can access it. Scrutiny of owned and leased systems that process critical data, including through cloudbased applications, and to the technical and organizational controls in place to protect such data, is often a key point of internal risk assessment together with the contractual relationships supporting those systems. While that exercise may be familiar, the need to act on information is evolving. An emerging development is the criticality of ensuring that teams have the tools and skills to report and act upon incidents promptly. Current operational best practices include maintaining an incident response plan and conducting annual training regarding the plan.

The importance of the transportation and logistics industry is increasingly under review from a global competitiveness, national security, and domestic safety perspective. This is positive for a segment that has long viewed itself as the "backbone" of the U.S. and, at least since the COVID-19 pandemic, is widely known across the country as holding that role. Along with that newfound visibility and esteem comes a call to action. The industry, like many other sectors, must remain on guard against the crippling effects that could all too easily be brought about by our enemies.