CONTRIBUTED CONTENT & PRESENTATIONS

Cybersecurity Protocols Emerge for the Transportation Industry

NOVEMBER 14, 2022

Authors: Jonathan R. Todd, Megan K. MacCallum

Cybersecurity has emerged as a tangible risk for transportation service providers over the course of the last year. Ransomware attacks on domestic industry and critical infrastructure, and tensions associated with the Russian invasion of Ukraine, are now ever-present reminders of technology's role in our businesses and the crippling risk of outside threats. The transportation sector as well as its regulators are taking notice.

In May 2021, criminal hackers launched a ransomware cyberattack on the American oil company, Colonial Pipeline. The attack on this often-overlooked means of surface transportation resulted in a multimillion-dollar ransom payment in just hours. The impact was operational as well as financial and reputational in nature, with a reported six-day shutdown of the companies operating systems. For the remainder of 2021, transportation regulators publicly ramped up directives around cybersecurity in an effort to raise industry awareness and instill best practices.

The lead time gained during the events of 2021 were not wasted in early 2022. Urgency of cybersecurity matters, and particularly their impact on the global supply chain, rocketed once again to the forefront with events in Ukraine. The U.S. Cybersecurity and Infrastructure Security Agency (CISA) recently issued a public warning regarding the risk of Russian cyberattacks on impacting U.S. networks in retaliation for sanctions against Russia. The European Central Bank (ECB) likewise expressed concern about potential retaliatory attacks on European financial institutions and markets. More recently, on March 21, 2022, President Biden reiterated these warnings. In an official statement, he revealed U.S. intelligence that indicates Russia is considering engaging in cyberattacks against the U.S. in the near term. President Biden referred private-sector players to CISA's "Shields Up" effort to assist organizations across the board to prepare for and respond to cyberattacks in the wake of Russia's invasion of Ukraine. President Biden urged private-sector players to strengthen cybersecurity immediately.

Domestically, the Transportation Services Administration (TSA) has stood at the forefront of the cybersecurity issue for the transportation sector. The TSA issued a Security Directive under its emergency authority [49 USC § 114(*l*)(2)(A)] following the Colonial Pipeline attack. 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: (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.

Transportation industry segments outside the pipeline space were not immune from risk or the TSA's attention. A few months later, the TSA issued similar directives for other segments, including the railroad industry, and for public transportation. The published Security Directives were designed to target higher-risk 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 White House is itself taking notice of the cybersecurity threat in our industry. The Biden-Harris Administration recently announced the introduction of its Freight Logistics Optimization Works initiative (FLOW). The initiative is 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 for participants. The objective is to reduce COVID-type disruptions and also to guard against interference through cybersecurity vulnerabilities and other threats. The initial participants in FLOW are reported to include the Ports of Long Beach and Los Angeles as well as the Georgia Ports Authority, terminal operators, private businesses, and logistics and warehousing providers.

More recently, President Biden signed the Cyber Incident Reporting for Critical Infrastructure Act into law on March 15, 2021. The Act will apply broadly to covered entities identified as critical to infrastructure across sectors. The Act will require that covered entities report certain cybersecurity incidents to CISA within 72 hours, and report ransomware payments to CISA within just 24 hours. The full application of the law will be further detailed in CISA regulations.

Initiatives such as the TSA Security Directives, FLOW, and the Cyber Incident Reporting for Critical Infrastructure Act are early examples of how we will be thinking about these cybersecurity issues for the foreseeable future. In the interim, it is clear that the operational effect of these efforts requires, by best practice or mandate, increased vigilance within the transportation industry. Beyond worrying about on-time delivery, it is time to also give attention to building tech-savvy teams who can conduct nuanced vulnerability reviews as well as reporting and acting upon incidents promptly. This is of course a tall task because the transportation and logistics business itself is a challenge. Cyber is nonetheless emerging as mission critical for all aspects of our business-from customer service and operational performance to regulatory compliance and national security.

Jonathan Todd is a partner in Benesch's Transportation & Logistics Practice Group whose practice includes advising clients on technical aspects of transportation operations and regulatory compliance. Jonathan may be reached at (216) 363-4658 and jtodd@beneschlaw.com. Megan MacCallum is an associate in the Transportation & Logistics Practice Group who may be reached at (216) 363-4185 and mmaccallum@beneschlaw.com.