Hogan Lovells

Staying Ahead of the Hack: New Cybersecurity Requirements on the Horizon for Trains and Planes

9 November 2021

Imagine a country paralyzed by the inability — even for just one day — to move people or goods by rail or by plane. This is not science fiction. This is the reality of the potential cybersecurity threats that could impact the transportation sector and its critical infrastructure. As companies continue to take a hard look at their own cybersecurity readiness, the United States (U.S.) Transportation Security Administration (TSA) is turning its focus to the rail and aviation sectors to make sure they're up to the task.

"Cybersecurity" used to be a buzzword uttered mostly by IT professionals, computer geeks, and hackers. In the wake of the past decade's mega-breaches — including the now-infamous 2013 Target data breach through which criminals stole over 100 million customers' financial data, the Yahoo! data breaches that compromised a billion or more user accounts, the Marriott/Starwood cyberattack that exposed up to 500 million guests' information, and similar incidents — seemingly everyone now knows about the need to protect passwords, ward off software intrusions, and keep networks and systems safe from all kinds of potential threats.

But today, "cybersecurity" has taken on an even-more-vital relevance given the proliferation of interconnected systems, critical services, and sensitive data driven in part by the Internet of Things. In fact, the U.S. government and others have been working to focus attention on critical infrastructure cybersecurity for years. But only when Colonial Pipeline, the owner of the largest fuel pipeline in the U.S., was attacked in a ransomware hack this summer did cybersecurity become top of mind for everyone—whether you're connected to the internet or not.

The Colonial incident demonstrated something that cybersecurity professionals have known for years: hacks — even ransomware attacks — are not just about stealing money or information. Hackers, whether criminals, state actors, or otherwise, may have the power to shut down electricity grids, empty oil, gas, or chemical pipelines, breach dams, infiltrate water supplies, derail trains, or wreak havoc in aviation. The energy sector knows this reality all too well. Now, the government is expanding its regulatory reach to cybersecurity preparedness in the rail and aviation industries.

What we learned from the Colonial hack

Hackers reportedly accessed Colonial through one compromised password. Although the ransomware didn't itself give the hackers access to Colonial's pipeline technology, the company shut down its services as a precaution. The headline: hackers may have been able to access the pipeline system, exposing potential vulnerabilities of our critical infrastructure. In the wake of Colonial, the TSA, an agency under the Department of Homeland Security umbrella, was empowered to regulate pipeline companies' cybersecurity efforts. TSA's efforts to date have included the issuance of two Security Directives, through which TSA has mandated a multitude of compliance initiatives that have forced numerous pipeline companies whose "critical" pipelines are subject to the new regulations to spend thousands of hours and millions of dollars upgrading, updating, and upscaling their cybersecurity protections.

TSA's new focus on cybersecurity for rail and aviation.

Now, TSA is on the verge of requiring similar compliance of rail and aviation companies. See https://about.bgov.com/news/tsa-launching-cybersecurity-requirements-for-rail-aviation/; https://www.zdnet.com/article/new-cybersecurity-regulations-released-by-tsa-for-trains-and-planes/; https://www.cnn.com/2021/10/06/politics/tsa-cybersecurity-mandates-railroad-aviation/index.html. And, although the some members of Congress have expressed that TSA should utilize notice-and-comment rulemaking in lieu of issuing Security Directives, there is little doubt that, in one form or another, regulation is coming. The immediate focus is on railroad operators, rail transit companies, U.S airport operators, passenger aircraft operators and all-cargo aircraft operators, but the supply chain should anticipate scrutiny as well — whether directly from TSA or indirectly through increased pressure on regulated customers. With the increase in scrutiny, regulated customers will have the expectation that all members of a supply chain will be aware of everyone else's security profiles and vulnerabilities.

Fortunately, Hogan Lovells — through its industry-focused, intermodal, and well-fused teams of multi-disciplined practitioners — has been helping clients navigate TSA's new cybersecurity directives since before they were released. To date, Hogan Lovells has assisted numerous large and small pipeline clients to overcome compliance challenges. Hogan Lovells lawyers are well-positioned to do so because they have one-on-one connections with TSA as well as other key government actors (including in law enforcement and cyber leadership) and know the world of cybersecurity intimately. From circuits to servers, from nation-state attacks to ransomware, and from workstation protections to tabletop exercises to board-level decisions, Hogan Lovells lawyers have extensive experience with cybersecurity issues and TSA's cyber regime. And we know the transportation sector and how it works. We can bring that experience to assist our rail and aviation clients tackle the latest cybersecurity challenges and anticipated regulations.

Authors

Emily Kimball
Counsel, Denver
T +1 303 454 2549
emily.kimball@hoganlovells.com

Andrew Lillie
Partner, Denver
T +1 303 899 7339
andrew.lillie@hoganlovells.com

Paul Otto
Partner, Washington, D.C.
T +1 202 637 5887
paul.otto@hoganlovells.com