CONTRIBUTED CONTENT & PRESENTATIONS

Beyond Care, Custody, and Control: Data Security Best Practices for the Transportation and Logistics Sector

SEPTEMBER 15, 2017

Authors: Jonathan R. Todd

The receipt, storage, and handling of sensitive shipper data occurs, often frequently and in real-time, alongside the flow of goods. Commercial shippers are well aware of the supply chain security risk to the materials and finished products tendered for transportation. Service providers are keenly aware of the commercial and legal risk to their own enterprises inherent in the safe movement of shipper tender. However, the security risks associated with data flows is a very real threat for both shippers and service providers that likewise deserves due attention.

Shipper data may include a broad range confidential and proprietary information, including strategic sourcing details (suppliers, inputs, and costs), account and sector details (customers, industries, and regions), and in today's e-commerce world the personal information of individuals (names, addresses, and contact information). It is easy to see how breaches in data security threaten to harm public relations, trading partner relationships, and competitive advantage with effects that will reverberate throughout the supply chain. Data security also carries the gravity of significant legal liability to those parties who disclosed or have an interest in the underlying data.

In the cybersecurity world it is often said that the risk of a security incident is "not an if, but when" question. Transportation and logistics companies collect, use, and maintain significant volumes of sensitive data just like the industries we often see in the headlines that encounter security breaches. Planning and preparation are the keys to weathering the storm. The very first source of information that government enforcement agencies or plaintiffs' attorneys will look to in the event of an incident are the corporate policies and procedures documenting data handling and security.

The best practice for transportation and logistics companies is to periodically review and update internal data handling policies and procedures to ensure compliance with the state of law and commercial standards. A comprehensive review will involve identifying and examining: (1) the receipt of critical data including any personal information; (2) the employees, personnel, and contractors who may have access to that critical data; (3) the owned and leased systems that process critical data including any cloud-based applications; (4) the technical and organizational controls that are in place to protect critical data from unauthorized access, loss, destruction or misuse; and (5) the legal, regulatory, and contractual requirements for handling critical data.

It is time to make informed decisions about how to mitigate identified risks of processing after arriving at a clear understating of internal practices. This step typically involves knowledgeable and pragmatic risk assessment including gap analysis. Even today, it is not uncommon to identify significant areas for improvement. Attorneys experienced in these technical areas draw from a toolbox of risk-prevention measures that may include:

- **Maintaining an Incident Response Plan.** Data breaches and security incidents to network systems maintained can occur at any time, whether on accident or by nefarious actors (including a disgruntled former employee). A documented incident response plan and procedure will prepare for these types of situations. The incident response plan should address incidents internal to the organization and incidents that occur involving third party service providers processing such information.

  –

- **Ensuring Accuracy of the Privacy Policy.** A privacy policy is a company's explanation of how it collects, stores, and uses high-risk personal information. A review of the published privacy policy and website terms of use will help to ensure they are truthful and non-deceptive by accurately reflecting the collection and processing of personal information.

- **Restrict Access to Data.** No employees, personnel, or contractors should have access to critical data unless they need that data to perform their day-to-day jobs. A process to periodically review system access lists for appropriateness, including revoking the credentials of those no longer needing access, is a periodic security measure to responsibly control risk.

- **Encrypt Sensitive Data.** One of the best ways to secure information at rest or in motion is through adequate encryption. Not only may encryption properly protect sensitive information, it may also relieve the company of any notification obligations upon a security incident. Each company that possesses high-risk data will benefit from evaluating technical solutions to address the need for encryption. For example, developing a data classification policy may reduce the costs of encryption relative to encrypting all data. Encryption can also be tailored to contractual requirements, which increasingly include encryption requirements before data is sent to a third party - even before hosting by cloud service providers.

Commercial shippers and their service providers are continually adapting to emerging threats and changing expectations, as well as the ever-evolving landscape of international, domestic, and local privacy and data security laws. Company-wide data security and privacy compliance reviews are essential to remaining vigilant by improving upon internal data security and privacy compliance programs as well as the expectations for trading partners. Like the safe movement of goods, data security is a constant concern of all supply chain participants because the reputations, growth potential, and legal liability of each can easily suffer from outdated practices.

Jonathan Todd is Of Counsel with the national transportation and logistics practice group of Benesch, Friedlander, Coplan & Aronoff. He may be reached at 216-363-4658 or jtodd@beneschlaw.com. **Justin Clark** is an Associate with the firm's innovation, information technology, and intellectual property group. He may be reached at 216-363-4616 or jclark@beneschlaw.com.