DAT iQ Analytics

Driving Digitalization with DAT iQ

Securing your supply chain

Keeping your connected supply chain secure

Connecting freight networks has opened many doors for shippers, carriers, brokers — and cybercriminals. As organizations continue to optimize, automate, and streamline their supply chains, they must take steps to safeguard their business as well.

In 2022, the FBI's Internet Crime Complaint Center (IC3) received more than 800,000 cybercrime-related complaints, with total losses related to these incidents exceeding $10 billion.

Department of Justice

The number of documented supply chain attacks increased by 600% in 2022.

CSO Mag

Shippers, brokers, and carriers face serious security threats while managing large, valuable pallets of in-demand goods. Trailer theft, identity theft, fraud, hijacking, and burglaries are all common within the industry, putting people and finances at risk. However, as transportation and logistics has become more connected through supply chain digitalization, shippers are in unfamiliar territory with the rising threat of cyberattacks.

A target on transportation's back

Digital transformation has changed the way that shippers, brokers, and carriers operate. By connecting their fleets, facilities, and equipment, businesses have discovered opportunities to optimize networks, open new lanes, eliminate waste, and improve their customer service options. Unfortunately, these benefits may create significant risks for fleet operators, the shippers that work with them, and the public, as cybercriminals capitalize on three intersecting factors:

Speed

As enterprise systems grow, they become increasingly vulnerable. The larger and more complex the system, the more likely there will be openings for attackers to exploit and the harder it is to monitor for disruptions. The breakneck speed of shippers' cloud migration further exacerbates that complexity.

Digital immaturity

Shipping's digital revolution is years behind the rest of the business world. Supply chain digitalization technologies only became available to shippers within the past decade. That means most shippers are:

1. Using Internet of Things (IoT) devices to integrate legacy trucking and manufacturing equipment into their systems.

2. Leveraging understaffed IT teams that often lack training on the nuances of protecting operational technology (OT) environments against cyber-physical threats.

Importance

For most people, the term critical infrastructure conjures images of power plants or water treatment facilities, but truckload shipping — which plays a role in 72% of the country's deliveries — has been an integral piece of the modern supply chain for decades. That makes transportation and logistics companies desirable targets for ransomware actors hoping the threat of disruption will force businesses to pay out enormous sums.

However, there's another risk that comes with digitalized integration: attacks through the supply chain. As more shippers, carriers, brokers, partners, and other entities integrate across company lines, the more they're at risk. Without the right protections, it only takes one vulnerability in one system for a hacker to move through privileged environments undetected and reach their desired target. On average, software supply chain attacks go unnoticed for 235 days after the first entry point.

Best practices for strengthening security

The good news is that other industries have been working to address cybercrime for many years. Shipping leaders can look to them for guidance on how to mature and strengthen their OT and IT security programs to meet the moment:

1. **Learn your systems**

   The first step is gaining a firm understanding of how your company's network operates both in isolation and with other systems. Leaders should assemble a cross-functional team of operations, cyber, and logistics experts from within the business. If you lack in-house OT or IT cyber expertise, it may be worthwhile to tap external experts or ask your data, technology, or other partners for guidance.

   The team should conduct an asset audit that notes every connected tool in your supply chain ecosystem and how it connects to other equipment. This will help identify vulnerabilities and the controls needed to prevent them.

2. **Learn your supply chain ecosystem**

   Connected supply chains are only as secure as their weakest link. Conducting robust partner assessments will show how their vulnerabilities could become a risk to your business.

   This also means assessing the features of the software suites you already use to see if they incorporate adequate protections, like:

   - Multi factor authentication (MFA)
   - Password strength requirements
   - Lock-out options
   - Fraud reporting
   - Protections for use on personal devices
   - Active monitoring

3. **Invest in the right tools**

   Once you understand your systems, you can begin to invest in tools and solutions that address the vulnerabilities within your warehouses, manufacturing facilities, fleets, and offices. This may mean considering other technology partners, investing in internal cyber monitoring and remediation tools, investing in end-to-end supply chain suites, or upgrading legacy equipment that isn't cut out for connected operations.

4. **Train your people**

   Research shows that nearly 70% of all breaches start with an employee clicking on a malicious link. Employee error is the most likely way hackers will gain access to your operations. Require training programs that teach employees to spot scams and fraud attempts to safeguard the organization.

5. **Prepare for the worst**

   In today's connected world, the question really isn't if you'll fall victim to an attack, it's when. No cybersecurity program is complete without specific protocols to prepare for attacks. These plans should include remediation steps for various OT and IT cybercrime scenarios identified in the audit, as well as plans for communicating about the incident with stakeholders, employees, and the public.

Fighting fraud and breaches with DAT

DAT understands the complex landscape that shippers face. We take the privacy and security of our data and that of our partners seriously. That's why we:

- Require multi-factor authorization on all DAT accounts
- Pursue continual improvement in fraud monitoring through our data science team
- Conduct regular testing to identify vulnerabilities
- Engage in an ongoing partnership with the FBI

Our Fraud Protection Program and dedicated Network Integrity Unit works to prevent malicious actors from gaining access to DAT iQ's network. We also provide security-focused tools to help users to quickly and accurately vet potential business partners, like:

CarrierWatch, which enables shippers to monitor changes in motor carrier authority, safety ratings, insurance status, and more for over 50,000 carriers.

DAT Directory, which provides customer contact information including phone numbers, addresses, DAT numbers, and more.

DAT One Tracking, which allows shippers to see exactly where their goods are to help teams stay ahead of bad actors.

Invoice factoring, which shows loads that have been pre-approved for factoring.

Contact us today or visit our website to learn more about how DAT is working to safeguard supply chains.

DAT iQ Analytics

www.DAT.com