EXPERT INSIGHT

CYBERSECURITY: UNDERSTANDING YOUR RISK AS A LOGISTICS SERVICE PROVIDER (LSP)

This guide explores policies and tactics organizations can adopt to be proactive in their approach to cybersecurity.

CHAPTERS

Introduction

Cyberattacks are frequently in the headlines, from ransomware demands that cripple companies' operations to critical data breaches that expose confidential information. Whether forcing the world's largest meat processing company to pay an $11M ransom, or exposing the credit card details and passport numbers of millions of hotel guests (twice!), cybercriminals threaten businesses of all sizes, across all industries and geographies—and show no signs of de-escalating their assaults.

The logistics and transportation sector has also faced cyberthreats with attacks on the rise. The good news is that many logistics-oriented companies now recognize the importance of cybersecurity and are taking steps to safeguard operations. This eBook provides an overview of the cybersecurity landscape, why logistics service providers in particular are a target, and what best-in-class businesses are doing reduce risk with best-in-class technology.

68% of business leaders feel that cybersecurity risks are increasing, highlighting the need for business leaders to take action now.[1]

1. Accenture

CHAPTERS

Cyberthreats 101

Cyberattacks against companies and governments take **many forms**: ransomware; malware; distributed denial of service (DDoS) attacks; **social engineering**—the manipulation of someone to divulge confidential information that can be used for fraudulent purposes—such as phishing, baiting, or scareware; and numerous other techniques.

Ransomware attacks—when hackers lock files on a device and demand a ransom be paid in order to unlock them—continue to be the **number one threat** to large and medium businesses. The uptick in ransomware attacks is also reflected in the logistics sector causing a cascading impact across the global supply chain. In fact, attacks are up almost **300%** since 2020 in the U.S., with $350M paid out in ransom in 2020; ransom damages exceeded $20B globally in 2021, with an average cost to companies of $5M.

The average breach cycle is **287 days** (212 days to detect an attack, 75 days to contain)—one week longer than last year. Plus, for those companies with a 50% remote workforce, the cycle takes an additional 58 days, on average.

Cyberattacks are sophisticated, can take many forms, and can have a high financial impact.

CHAPTERS

The state of the transportation cybersecurity landscape

In the midst of supply chain disruptions, sanctions, and global instability, the transportation industry is increasingly becoming a target for cybercriminals. Indeed, the frequency and severity of cyberattacks is on the rise, with the transportation industry moving from ninth place ranking in 2020 to **seventh** on the list of most attacked industries in 2021.

The attacks are hitting close to home: a recent cyberattack on a Global Top 10 Forwarder limited its ability to book freight electronically; hackers targeted 10,000 mailboxes in **phishing attacks** on Global Parcel Integrators in February 2021; a 2021 data breach for a Top 25 Global Forwarder; and a top US Based third-party logistics provider (3PL) suffered a **ransomware** incident that affected its operational and information technology (IT) systems, causing service delays and resulting in the loss of an estimated $7.5M of less-than-truckload (LTL) revenue. Cybersecurity experts warn that it's not if your organization will be attacked, but when.

Logisitcs service providers are increasingly becoming targets for cybercriminals.

CHAPTERS

Why are Logistics Service Providers (LSPs) a target?

While cyberattacks on the transportation sector have always occurred, the world today has a greater-than-ever reliance on logistics companies to ensure that supply chains keep flowing in the face of increased consumer demand, congested ports, truck driver shortages, and other supply chain disruptions. Hackers are capitalizing on this dependence and exploiting the inherent vulnerabilities in logistics and supply chain operations and infrastructure.

Unfortunately, LSPs are easier targets for attack because many rely on legacy systems built 10, 20, or even 30 years ago, spread across a broad geography; governments are part of the problem as well, often running programs that are 20+ years old.

Indeed, cloud and SaaS solutions have not yet been entrenched in the logistics industry and relying on legacy systems—many that still run on AS/400's—to support our global supply chains is problematic. Adding fuel to the fire, many companies continue to rely on a patchwork of different IT systems to conduct business electronically, creating vulnerabilities that increase the risk of a costly attack.

The logistics industry is also a rich source of data for cybercriminals. From customer relationship management (CRM) solutions, governmental declarations, and connections to third parties (e.g., carriers) to accounting and pricing data for customers, importers, and shippers, LSPs manage a sizable repository of data. Plus, logistics companies send and receive copious amounts of data on a daily basis, creating the need to secure not only *data at rest* but also *data in flight*.

CHAPTERS

What could a cyberattack cost your organization?

The global cost attributed to cyberbreaches was $6 trillion in 2021—up more than $3T from 2015. According to a 2021 cybersecurity study by Ponemon Institute and IBM Security, the average cost per data breach was a staggering $9.05M in the U.S., compared to a worldwide average of $4.24M per incident—the highest cost in the 17-year history of the report.

The transportation industry was ranked as the eleventh most costly sector for experiencing a data breach, with the cost per breached record averaging $130. Given that most LSPs manage hundreds or thousands of customer, partner, and employee records, these costs can add up quickly.

In addition to lump sum payouts associated with a ransomware attack, consider the following costs that could impact your organization following a cyber incident:

Replacement of IT Assets/ Infrastructure

Impact on Credit Rating

Reputational Damage

Potential Litigation or Legal Fees

The Cost of IT Forensics

Government Penalties or Fines

CHAPTERS

How vulnerable are you?

No organization likes the thought of hackers making themselves at home in their company's computers and systems for, on average, 180 days and learning everything about their business—who they email, their company financials, which partners and customers they have relationships with—but it happens every day, all over the world.

To determine the extent of your vulnerability to a cybersecurity attack, LSPs should begin by taking a data security self-assessment:

- Do you know your full technology footprint? What age are your servers and the releases of software – both operating systems and applications?
- Does your organization regularly monitor release updates to see what enhancements have been made to improve system security?
- Is your software currently supported and does your software provider have modern security practices in place?
- How much of your software was built in-house and do you still have the documentation and resources who built the custom software?
- Does your systems infrastructure help prevent the spread of attacks across applications and organizations?
- Do you use secure connections to partners? Do you often use FTP?
- Is your IT or development outsourced? Are you aware of security measures being taken by your outsourced contractors?
- Are your systems in a secured data center or a back room at your operations?
- Do you have a Business Continuity Plan (BCP)? When was it last updated?
- Who 'owns' or champions cybersecurity in your organization?

CHAPTERS

Calls to Action

Ask yourself honestly how well you did on the self-assessment. If you answered 'No' to any more than one or two questions, your organization is at a high risk of being compromised with potentially devastating results.

If your cybersecurity self-assessment revealed risk, it might be time to consider further questions such as:

- As an LSP, are you willing to continue to invest in legacy and/or proprietary systems?
- What technology partners do you have today that can offer you a secure environment?
- Have you had an external (third-party) security assessment done on your organization?
- What level of risk are you carrying across your logistics operations worldwide and are you willing to lose customers if a hacker disrupts your business?

Minimizing the risk of a successful cyberattack

For LSPs, mitigating the risk of cyberattacks requires top-down buy-in, a true commitment from leadership to develop a culture of security. Ideally, LSPs should appoint an individual or department to focus on cybersecurity. As a starting point, consider the cyber anti-patterns put forth by agencies such as the U.S. Cybersecurity & Infrastructure Security Agency (CISA).

This short list of cybersecurity bad practices outlines the basics of what *not* to do:

- Don't run unsupported or end-of-life software
- Don't run software that has not been recently updated or patched
- Never have a single factor authentication for important control systems exposed to the Internet

CHAPTERS

Adopt Accepted Cybersecurity Guidelines

In order to reduce risk, LSPs should consider the five pillars of NIST's Cybersecurity Framework to minimize the risks to their organization:

Identify

Locate and catalog assets and related cyber risks. Develop an organization-wide understanding to manage cybersecurity risk to systems, assets, data, and capabilities.

Protect

Immediately guard and quarantine any points of risk. Develop and implement an immediate plan to ensure continued delivery of critical infrastructure services.

Detect

Pinpoint where, when, and how the breach occurred. Develop and implement activities to detect and notify IT security of subsequent attacks.

Respond

Implement safeguarding protocols to prevent and quarantine future potential events should they occur.

Recover

Develop or update plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity event.

CHAPTERS

Conclusion

The logistics industry is highly inter-connected with business partners and operations across multiple countries. An interruption of services due to a cyberattack can not only disrupt internal processes but can bring the movement of freight to a standstill.

However, according to a 2019 Eye for Transport (EFT) report, at least 55% of logistics employees feel that they are ill-equipped to handle or even identify a significant cyberattack. Beyond this, only 43% of trucking and logistics companies have a Chief Information Security Officer (CISO) championing for security—and only 21% of logistics companies believe they even need the expertise of a CISO.

Adding further risk, LSPs may use older technology that is no longer supported, with unplugged points of vulnerability, or that relies on outdated protocols. As hackers become more aggressive, LSPs must adopt proactive cybersecurity policies within an enterprise-wide, coordinated framework across multiple operational, technology, and strategic areas. They need to implement leading edge technology that uses the latest cybersecurity protections, screening, and automated notifications of potential threats. With modern solutions in place, LSPs are better positioned to reduce risk, decrease reputational damage, and minimize potential revenue loss.

CHAPTERS

How Descartes Can Help

Descartes is the global leader in providing on-demand, software-as-a-service solutions focused on improving the productivity, performance, and security of logistics-intensive businesses. We are helping LSPs move away from legacy technology that can be more prone to cyberattacks.

Our solutions are built upon the latest architecture using the Descartes Global Logistics Network™ (Descartes GLN™), which manages the real-time flow of information for thousands of LSPs. Our users benefit from:

- A modern application structure to safeguard against cyberattacks
- Denied Party Screening (DPS) across a frequently updated database of cyber criminals
- Advanced analytics to better understand logistics operations, including points of potential risk
- Alerts if a high-risk cyber-criminal is identified as part of a manifest, customs entry, or security filing across any mode of transport
- A 24/7 network operations center that responds to security events
- The support of Descartes' dedicated in-house team of IT Security professionals

Our long-term knowledge of the logistics sector means that we understand the global nature of LSP operations and the importance of Information Security to guard against potential cyberattacks. Descartes is helping to protect our customers as they move freight worldwide through our innovation, deep expertise, and commitment to IT security advancements.

Ask Us How We Can Help LSPs Reduce the Risk of a Cyberattack.

CHAPTERS

About Descartes Systems Group

Descartes is the global leader in providing on-demand, software-as-a-service solutions focused on improving the productivity, performance and security of logistics-intensive businesses.

Customers use our modular, software-as-a-service solutions to:

- Access global trade data
- File customs and security documents for imports and exports
- Route, schedule, track and measure delivery resources
- Plan, allocate and execute shipments
- Rate, audit and pay transportation invoices
- Complete numerous other logistics processes by participating in the world's largest, collaborative multimodal logistics community

Our headquarters are in Waterloo, Ontario, Canada and we have offices and partners around the world.

Learn more at www.descartes.com, and connect with us on LinkedIn and Twitter.

DESCARTES™

The Descartes Systems Group Inc.
120 Randall Drive, Waterloo, Ontario, N2V 1C6, Canada
Toll Free 800.419.8495 | Int'l 519.746.8110
www.descartes.com | info@descartes.com

Uniting the People & Technology
That Move the World

CHAPTERS