CYREN

10 Steps to Protect Your Logistics and Transportation Business

Solution Brief

Logistics and transportation companies of all sizes have become targets for phishing, malware, and ransomware attacks.

In a world increasingly dependent on digital technology and with supply chains becoming more interconnected, the logistics and transportation industry is being challenged by continued increases in the volume and sophistication of cyberattacks and the need to modernize their security to protect corporate assets and employees. Failure to do so can mean data theft, business interruption, financial loss, and reputation damage.

Industry Dynamics Increase Cyberthreat Risk

Extensive partnerships create collective risk – The decentralized and interconnected nature of the logistics and transportation industry makes email and web threats particularly dangerous. The distribution of a single container involves information and goods transfers with at least ten different stakeholders, including the shipper and consignee, shipping lines, ports, secondary distribution or shipping companies, as well as customs and border authorities if the item is shipped outside the country. Every entity involved in the supply chain communicates and connects with other partners, creating points of shared access and risk.

Smaller companies frequently the point of entry – Small and mid-sized companies are integral parts of the larger logistics and transportation cycle, and are frequently targeted in an effort to get at larger partners and customers, or find themselves affected as part of a broader supply chain attack. According to the 2018 Verizon Data Breach Report, small businesses are the target of cyberattacks more than 58% of the time.

A larger attack surface from increased digitization – The industry is becoming heavily reliant on internet-based operational processes and information transfer and sharing. This means more systems that could potentially be targeted and affected by attacks.

Geographically dispersed companies using disparate technological systems – Logistics and transportation involves multiple organisations all using different technologies to engage in business across different time zones and even countries. This results in an asynchronous technological and communications environment, where threats may take time to be discovered.

Unprotected mobile workforce – With an increasingly mobile workforce, employees are no longer confined to a work environment protected by perimeter security devices. Bring-your-own-device (BYOD) policies mean that numerous different devices, each with a different operating system are accessing company resources – and potentially downloading harmful phishing, malware, and ransomware that, in turn, gets passed to others on the same corporate network. Today, mobile devices need to be protected regardless of location, device type, operating platform, or device ownership.

Maersk cyberattack had far-reaching supply chain consequences

In June 2017, almost 100 ports and terminals around the globe came to a standstill or experienced significant delays, including major ports in Europe, the U.S., South America, and Asia, as a result of a malware attack on the Maersk shipping company. All operations, including related supply chain activities such as trucks arriving at the ports for shipment pick-up or delivery, were held up for hours and even days as businesses waited for the systems to come back online.

The attack on Maersk's computer systems ended up costing the company an estimated $300 million. And, with no way to clean the infected computer systems, Maersk had to rebuild a significant portion of its IT infrastructure, installing over 50,000 new PCs, servers, and applications over the next two weeks.

Analysis of the Maersk attack suggests that the incredibly complex logistics and transportation supply chain is partly to blame. The infection of Maersk facilities and ships by the NotPetya ransomware was likely the result of an initial attack on Ukrainian businesses. Maersk and others were simply collateral damage in the wider complex supply chain.

> “More than 60% of cyberattacks originate from the supply chain or from external parties exploiting security vulnerabilities within the supply chain.”
>
> **ACCENTURE, 2016**

25B	1.3B	300M
Security Transactions Daily	Users Protected	Threats Blocked Daily

10 Steps to Protect Your Logistics and Transportation Business

Solution Brief

The Business Impacts of a Breach

Among the potential business risks that logistics and transportation businesses need to factor into security decisions are:

Business interruption – Logistics and transportation businesses are heavily reliant on project and production schedules to ensure profitability and customer satisfaction. It only takes one ransomware attack to have a detrimental effect on an entire supply chain distribution process, including work stoppages and potentially significant delays in the delivery schedule. In the 2017 Maersk attack, it wasn't only maritime ports and container vessels that were affected. Trucks destined for ports with deliveries or pick-ups were held up for hours and even days at various ports waiting for the systems to come back online.

Significant financial loss – Malware can cause major financial damage by temporarily or permanently ruining computing systems. In the case of the NotPetya attack, many companies, including Maersk were unable to retrieve their systems, requiring the purchase of new computers, servers, and software. In addition, a phishing attack on a logistics or transport company that has just received a large payment for a service or delivery, could result in a sizable sum of money going missing from a bank account.

Loss of sensitive corporate data – Phishing attacks, including spearphishing or business email compromise (BEC) attacks use spoofed email messages and copycat websites that look legitimate to trick victims into sharing valuable personal or business information, such as personal identification numbers, user names and passwords, or even operational information, such as navigational data or signal equipment.

Loss of reputation and business – Logistics and transportation companies risk major reputation damage and loss of clients and business if their company is used as the point-of-entry for a larger cyberattack. As an industry that operates with a large number of stakeholders, cybercriminals may use small stakeholder businesses, such as a small transportation vendor to initiate a hack. This hack may aid the successful breach of a larger supply chain stakeholder, or shut down an entire logistics operation because one link in the supply chain is broken.

What you can do to protect your company, business partners, and customers

1. **Automate threat updates to the shortest possible time interval.** You need to make sure there isn't a time lag for protection from new threats.
2. **Deploy cloud-based email gateway protection from a security provider.** Cloud-based secure email gateways add more advanced security like time-of-click URL analysis and protection from business email compromise. The default security provided by hosted email security services like Office 365 provides only a basic layer of protection.
3. **Deploy a web security gateway.** An effective web security gateway will stop new and zero-day malware downloads, attempts to access malicious URLs, and communications with botnet C&C servers.
4. **Protect against evasive threats with sandboxing.** Today's malware developers are incorporating many different tactics to evade detection by traditional technologies. A cloud sandbox array is a new capability that can sit in-line with an email security gateway to protect from today's evasive malware.
5. **Use a password management tool and multi-factor authentication.** Password re-use makes phishing attractive for criminals. A breach into one system containing user names and passwords will likely be exploited to access other systems.
6. **Deploy endpoint security with active/behavioral monitoring.** Malware and ransomware evolve quickly and you need to augment traditional AV with next-generation detection.
7. **Patch early, patch often.** Outdated operating systems, browsers, and plugins are major vectors for malware infections.
8. **Back up regularly and keep a copy off-site.** If your files are ever encrypted by ransomware, then you can simply restore them after removing the ransomware. You should test that your backups can be restored-don't wait till an emergency!
9. **Turn off network shares and unnecessary admin rights.** Current malware exploits sharing vulnerabilities and seeks out mapped network drives with large file repositories. Also, some malware leverages admin privileges.
10. **Train users.** Educate users about the social engineering tricks that are used.

Consult us about Cyren's security services:

Email Security Web Security Cloud Sandboxing DNS Security

www.Cyren.com sales@cyren.com