7 Ways to Improve Your Logistics Company's Cyber Security in 2021

Are you looking for ways to improve cybersecurity for your logistics company in 2021? Yes? You're in the right place.

Did you know that only 21% of logistics companies polled for the 2019 State of Logistics Technology Report believe they need a Chief Information Security Officer (CISO)? With that said, 35% of service providers and 43% of shipping firms actually had a CISO in place.

Unsurprisingly, 55% of logistics personnel cited feeling ill-equipped to identify and handle cyberattacks. What this demonstrates is that the state of awareness of the role of cybersecurity within the logistics industry is still relatively low.

However, the recent spate of attacks on logistics firms has now finally got the attention of companies, and we are beginning to see growing interest in improving cybersecurity within the logistics industry.

Here are seven innovative ways to boost your network security initiatives in the New Year.

1. Increase security awareness within the organization

Ensuring the company is safe is not solely the mandate of the IT department. Everyone connecting to the internal network plays a role in maintaining a safe cyber environment. Lack of security awareness is one of the biggest challenges that IT teams struggle with when trying to improve cybersecurity within logistics companies.

In 2021, awareness must begin at the board room level and then trickle down to the employees. If the CEO, CFO, and board show their seriousness and commitment to preventing cyberattacks, a new culture of accountability and responsible use of the internet within the workplace can begin.

2. Identify and patch vulnerabilities within your enterprise

The second step to improving cybersecurity within your logistics company in the New Year is identifying risks in your current operations and plugging them.

The widespread adoption of IoT and IT in the logistics sector has opened the door wide for threat agents to terrorize logistics companies.

To get an idea of the ramifications of a cyberattack, one only has to look at how multinational corporations such as shipping brokers AP Moller-Maersk were left paralyzed in 2017, following the NotPetya virus attack.

With 574 global offices situated in 130 countries and a massive fleet of 800 vessels, Maersk is the leading Maritime broker and logistics company. However, in spite of this, the NotPetya cyberattack brought operations to a grinding halt.

Cargo could not be processed and moved from warehouses, freighting trucks could not load and offload, and ships could not dock. It was a nightmare of apocalyptic proportions.

3. Segment networks and decentralized IT management

Technology has made it easier for companies with global operations to collaborate, exchange information, and communicate in real-time. However, this can also be a potential weakness in the event of a cyberattack.

When Chinese state-shipping firm COSCO suffered a network breach in 2018, it affected both on land crews and those on the open waters. Communication channels between ships and ground logistic teams were cut off. Customers were also left in the dark.

It has been argued that had COSCO's networks been segmented, it would have been easier to contain the attack. Network segmentation and decentralization of IT management are fundamental to securing networks. When the network is partitioned, it is easier to halt the spread of malware during an incident. The affected zone can be isolated and placed under quarantine, while remediation steps are taken.

4. Invest in robust encryption mechanisms

When it comes to improving cybersecurity within logistics companies, encryption mechanisms cannot be overlooked. Experienced IT teams are all too familiar with the need to implement strong encryption mechanisms as part of security efforts. Encryption, put simply, is the process of encoding data in order to block unauthorized access.

Now, this can be applied to internal communication and customer data so that in the event of a breach, the information cannot be used to blackmail the company. It is not uncommon that logistics companies are hacked as part of a ransomware attack, as happened in 2017 to British shipping and logistics broker Clarkson Platou.

5. Integrate strong identity authentication control systems

Segmenting networks is a great way to partition the internal system. However, more measures are needed to ensure that only authorized personnel have access to the company network.

This can be achieved through the thoughtful integration of identity authentication control systems. These access control mechanisms provide identification and authentication. Identification within the company will be provided by the IT team.

Identification is typically a username or email address that grants you entry into internal networks. Authentication is provided through a password. 2-factor authentication is now being widely adopted to help strengthen network security as well.

6. Hire the right talent to manage your cybersecurity needs

The cyber landscape has changed. The traditional IT perimeter has become more complex because it now features IT, OT, smart devices, and services spread out across supply chains.

Speaking at the SecureWorld Atlanta expo, Rebecca Herold aptly pointed out just how difficult managing today's perimeters is, "How many IoT devices exist, with how many computing devices do they share data? How many others have access to that data, and what decisions are being made with this data? No one really knows. We just don't know." These systems require suitably qualified personnel to handle them. Finding the right talent will go a long way in keeping your operations safe.

7. Select security products that meet growing perimeter requirements

Poorly secured IoT devices offer cyber terrorists an easy entryway into your network. You see, previous security products were designed for traditional IT requirements and don't offer comprehensive cover for OT as well.

There is a need to review, replace, and revamp your security products to ensure optimum cover. Systems must be updated and patched, and security products upgraded to match how fast technology is changing. Don't give hackers a free pass to attack your logistics company in 2021.

The bottom line

As more logistics companies move operations onto the cloud and adopt new technologies, there is a growing demand for ways to improve cybersecurity. Armed with these seven tips, you're well on your way to strengthening your enterprise's cyberspace.