SECURITHINGS

The Logistics Industry Faces Growing Physical and Cyber Threats...

Logistics companies are becoming increasingly attractive targets to threat actors because of the volume and value of the items they transport and the sensitive nature of the customer information they store and handle.

What are Logistics Companies up against?

Almost **$130 Million** of cargo was stolen in 2022

57% Spike in cargo theft in 2023 vs. 2022

$1.15 Million The average cost of a cyber security breach (in the transport and logistics industry alone)

Are Your Devices Properly Maintained?

On average:

8% of devices are misconfigured

57% are running on outdated firmware

In a typical week:

6% of physical security of devices are disconnected from their network

4% of cameras are disconnected from their video management system

Unmanaged Devices = An Open Door For Cyber Attacks

On the average physical security organization:

40% of devices are vulnerable to attack due to outdated firmware

15% of devices have reached their end of life, and therefore no longer supported by their manufacturers – including security patches

41% of cyberattacks exploit IoT device vulnerabilities

Weak device passwords are commonly exploited by attackers, due to unchanged manufacturer - set passwords and poor password security practices

The Need for an Effective Physical Security Solution

The need to maintain a robust physical security solution goes beyond the loss of cargo. At the end of the day, it's about the impact that cargo thefts have on people. That's why logistics companies need to operationally manage their devices consistently, making sure they run reliably.

So, What Can You Do?

With the SecuriThings platform you can gain full visibility and control of all your physical security devices and the power to respond rapidly whenever necessary, whether remotely or on site.

Improved system availability
Minimize device downtime. Get real-time data on device status and manage operational issues whenever they arise.

Ensured compliance
Ensure organizational compliance with automated maintenance processes set based on organizations' internal IT policies and relevant legal regulations.

Significant cost savings
Reduce manual labor and on-site visits, as well as other expenses related to managing physical security devices. Diagnose and resolve all issues, all in one consolidated platform.

Protection from cyber threats
Detect and prevent security vulnerabilities from compromising your devices. Automate crucial maintenance activities such as password rotation and firmware upgrades.

Visibility for future planning
Plan for device end of life, and prioritize your maintenance activities and budget accordingly.

Contact us to learn more **info@securithings.com.** www.securithings.com