

4 Ways eCommerce Businesses Can Protect Logistics And Warehouses

TechRounder PDF Edition

Live article:

<https://www.techrounder.com/business/4-ways-ecommerce-businesses-can-protect-logistics-and-warehouses/>

By Vipin PG | Published January 12, 2023 | Updated January 4, 2026 | Format: Article | 4 min read

In brief

As an eCommerce business owner, you must consider ways to cut costs and prevent losses. Warehouse shrinkage can cause drastic losses for your business, and you need to be looking to security to mitigate this risk.

As an eCommerce business owner, you must consider ways to cut costs and prevent losses. Warehouse shrinkage can cause drastic losses for your business, and you need to be looking to security to mitigate this risk.

So, how can you ensure adequate security protection at your logistics and fulfillment warehouses?

Keep reading as we list how eCommerce businesses can better protect their logistics and fulfillment warehouses against the modern security threat landscape.

Cloud-Based Access Control And Video Management Systems

When it comes to your physical security hardware, you need to stay on top of emerging trends that can improve the agility of your security operations. Cloud-based technologies are quickly dominating the security sphere and providing more convenience and agility for security teams responding to security threats.

Cloud-based access control and commercial building security cameras are some of the most popular options for security professionals. They provide remote management features that impact every facet of your security process.

Here are some of the benefits of implementing a cloud-based access control system at your logistics and fulfillment warehouses:

Increased visibility - your security staff and system administrators can view who has accessed the building. They can do this from anywhere at any time with cloud-based mobile applications, meaning they will always be up-to-date and aware of security occurrences, even off-site.

Remote operation - if you have a site visitor or a door is left unlocked, your security staff will be able to unlock and lock doors from anywhere remotely. With an on-premise system, they might need to travel to a control room or the building's entrance to open a door, which can be highly inefficient and time-consuming.

Integrations - cloud-based access control comes with open API integrations that allow logistics warehousing facilities to implement software solutions like visitor management systems and wellness verification software, automating processes to reduce time-consuming manual security processes.

When purchasing access control door locks, it's essential to understand the distinction between fail-safe vs. fail-secure door locks. Fail-safe locks require power to stay locked and, therefore, will unlock if the power supply is cut. Fail-secure locks require power to open and will remain locked if the power supply is cut. Understanding this distinction can help you to determine which strategy best suits your warehouse security.

Here are some of the benefits of a cloud-based video security management system:

Remote visibility - one of the critical flaws in a video management system is that security teams must be on-site and consistently monitoring video feeds to spot potential threats and investigate security incidents. Security professionals can access the video feed from anywhere using their mobile devices with a cloud-based system.

Integration - with cloud-based video surveillance, you can integrate access control and video management systems, making all security data readily accessible on a single user interface. In addition, unifying this data on a single platform allows identity verification without correlating timestamps from different data locations, which could slow down security response procedures.

Security Workflow Automation

When you opt for a cloud-based security system, you can improve project management for your warehouse security. You can apply threat detection software such as video and data analytics. These software solutions will provide your security teams with alerts on their mobile devices based on potential security risks.

To automate security response project management, you can ensure security personnel receives automated workflows in line with security alerts. You can establish response procedures for different types of security threats. When danger occurs, the system automatically generates workflows in line with these threats and assigns them to a team member for immediate action. Manual workflow assignments would take up critical time.

Converging Cyber And Physical Security Teams

If you wish to improve security operations for your logistics and fulfillment warehouses, it's time to stop thinking of cyber and physical security as separate concepts. Instead, cyber and physical security are essentially linked due to the introduction of cloud-based security data storage.

By merging your cybers and physical security teams, you can provide a security strategy that mitigates the following vulnerabilities:

Unauthorized access to cloud-based security resources - your cybersecurity team can implement cybersecurity protections to ensure your physical security data stays in the hands of authorized individuals. If a third party were to gain access to remote operation features for your physical security system, this could result in a critical cybersecurity breach.

Unauthorized access to on-premise digital resources - your physical security system protects your server rooms and digital assets from intruders. By merging cyber and physical security teams, you can ensure that both teams coordinate to keep your digital assets secure from a cyber and physical standpoint.

Integrate Cybersecurity Policies Into Physical Security Hardware

Zero trust is a cybersecurity policy that protects companies from internal security breaches and compromised employee accounts. It grants users only role-based permissions to access the data they need for daily operations. This way, even if an employee account is compromised, only a limited amount of data will be breached.

You cannot trust everyone on your network simply because they can access it - and the same goes for your physical security. Likewise, you shouldn't trust every visitor, interviewee, and contractor because they can access your building.

So, to mitigate the risk of a security breach, you should install security door locks to protect areas housing sensitive data, such as server rooms and any housing products and sensitive eCommerce assets. You should also apply video security to capture any events in these areas. Since employee theft is a significant concern in the warehousing industry, taking these precautions could significantly lower your exposure to inventory shrinkage.

Summary

Suppose you're looking to secure your logistics and warehousing facilities as an eCommerce business. In that case, you need to consider the benefits of cloud-based security and an integrated cyber and physical security approach. Consider the security tools and best practices listed in this article and how beneficial they would be for your security strategy.

References

1. pelco.com - solutions / industries - <https://www.pelco.com/solutions/industries/commercial/>
2. avigilon.com - blog / fail-safe-vs-secure - <https://www.avigilon.com/blog/fail-safe-vs-secure>