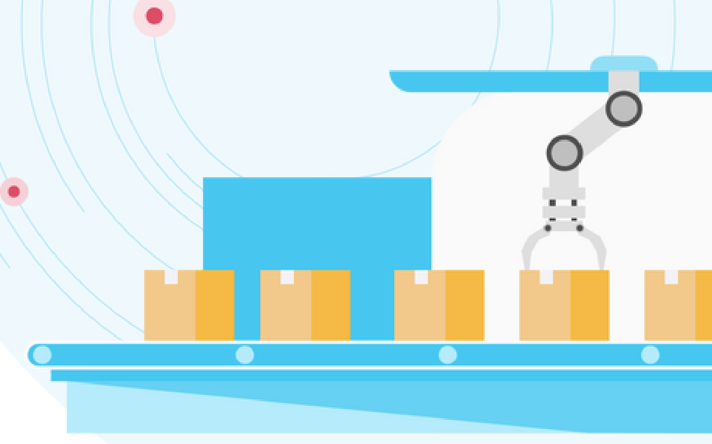
SECURITHINGS

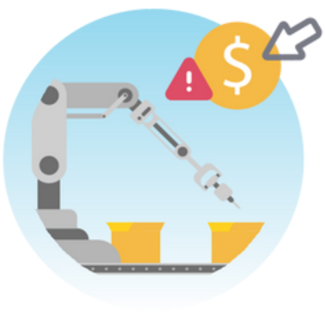


How Physical Security Device Downtime Leaves Manufacturers Vulnerable

Manufacturers must not only be concerned with safeguarding individuals from criminal activities but also with addressing risks such as workplace accidents, lawsuits, and penalties that can result from unsafe working conditions.

What are Manufacturers up against?

$50 Billion
The estimated cost per year of employee thefts within U.S. businesses



$8.98 Billion
The direct cost of a slip and fall accidents in 2023

$68.5 Billion
penalty costs for the Manufacturing industry for failing to comply with OSHA laws and regulations

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57% are running on outdated firmware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40% of devices are vulnerable to attack due to outdated firmware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, default passwords and poor password security practices

The Need for an Effective Physical Security Solution

At the end of the day, physical security managers' top priority is protecting people and assets – without leaving their organizations vulnerable to expensive lawsuits and fines. That's why physical security managers 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