SECURITHINGS

For Oil & Gas Companies, Automated Physical Security Device Management is Crucial

The oil & gas industry is not only faced with a wide spectrum of threats like environmental hazards, worker safety, deliberate acts like vandalism, theft, and terrorism, but it also has to grapple with securing vast facilities that often span extensive areas, making it difficult and expensive to detect those threats.

Are Your Devices Properly Maintained?

In the average physical security organization:

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57% are running on outdated firmware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

In 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40% of devices are vulnerable to attack due to outdated firmware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 Cost of "The Status Quo"

The Nord Stream Pipeline Explosion Case:

Sabotage is a serious threat as seen in the Nord Stream Pipeline explosions in 2022

$500 Million The estimated cost of repairing the damaged Nord Stream gas pipelines

The Colonial Pipeline Company Cybersecurity Incident:

$4.4 Million The ransom cost of the 2021 Colonial Pipeline Company cybersecurity incident

6 days The time it took to resolve the incident

More Stats From Other Cases:

$8.4 Trillion The global cost of a cybercrime in 2022

$11 Trillion The forecast cost of cybercrime in 2023

Working at an oil rig was listed as the **third most dangerous profession** in March 2023

The Need for an Effective Physical Security Solution

At the end of the day, the oil & gas industry's top priority is protecting people from dangerous criminal activities – while mitigating the potential for environmental hazards and ensuring worker safety. 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.