Digital Risk: Remote-Monitoring, IoT Sensors and Data Integrity Stats and Facts



FACTS

- **A Sensor Is Only as Reliable as Its Data:** A sensor that is miscalibrated, compromised, or malfunctioning does not report an unsafe condition — it reports a number. Workers acting on false data face hazards that are invisible until they become injuries.
- **Remote Access Is a Two-Way Door:** Systems that allow authorized users to monitor conditions remotely can also be accessed by unauthorized parties. Without proper authentication and firewalls, remote access is an open channel to every safety-critical system it connects to.
- **Data Integrity Is a Safety Issue:** Altered or falsified sensor readings can mask dangerous conditions — low oxygen levels, high chemical concentrations, equipment faults — until it is too late for a worker to respond.
- **IoT Devices Are Frequently Unmanaged:** Many industrial IoT sensors are not regularly patched or monitored for abnormal behavior, creating persistent vulnerabilities in systems workers depend on for safety information.
- **Automation Can Fail Silently:** A compromised or misconfigured safety system may continue to appear functional while providing no real protection. A green light on a dashboard is not the same as a confirmed safe condition.

STATS

- The average cost of a manufacturing sector data breach reached $4.97 million in 2024, not including regulatory fines and business interruption losses, according to industrial cybersecurity research.
- 77 percent of industrial firms remain in the initial phases of OT security implementation, with none fully secured, according to OT/IoT security industry research.
- 15.14 billion IoT devices are projected to be installed worldwide by 2029, significantly expanding the attack surface in safety-critical environments.
- On February 5, 2021, a hacker gained unauthorized remote access to the Oldsmar, Florida water treatment plant and increased sodium hydroxide

concentration from 100 to 11,100 parts per million — a level capable of causing severe chemical burns or death. An alert worker noticed and reversed it before it reached consumers.

- Manufacturing was the most targeted sector for ransomware in 2025, with a 58 percent year-over-year increase in victims across industrial organizations, according to GuidePoint Security.
- 34 of the 39 most frequently exploited IoT vulnerabilities have been known for more than three years on average — meaning most successful attacks exploit already-documented, preventable weaknesses, according to Asimily's 2024 IoT Device Security Report.