INDUSTRIAL CYBERSECURITY AND
RANSOMWARE FIELD REPORT

2026

PARAKEET

THE OPERATIONAL RISK

# INDUSTRIAL CYBERSECURITY

## HOW DIGITAL ATTACKS STOP PHYSICAL PRODUCTION

WWW.PARAKEETRISK.COM


PARAKEET

# THE FACTORY FLOOR IS INSIDE THE BREACH BLAST RADIUS

**This 2026 report explores rising cybersecurity threats in industries, focusing on manufacturing's growing vulnerability to ransomware.**

The recent data indicates a significant surge in attacks, where enterprise IT failures—such as compromised identities and remote access—frequently spill over to disrupt physical **production lines.**

Most breaches stem from common vulnerabilities like stolen credentials and **weak third-party controls** rather than specialized industrial malware. Despite these rising risks, a critical visibility gap persists, as many organizations cannot monitor the traffic between their corporate and operational networks. Bridging this gap requires real-time monitoring and quicker response times to any suspicious activities.

> *Addressing these trends demands a dual focus: optimizing monitoring efforts and safeguarding the infrastructure that ensures process resilience*

Collaborative efforts with third-party vendors to enforce stringent security standards are also essential, as these partners often form part of the extended enterprise network.

# CYBER RISK IS BECOMING PRODUCTION RISK

**How are ransomware, identity compromise, and third- party exposure turning ordinary IT failures into industrial disruption?**

The staggering figure of 1,020 industrial ransomware victims translates to millions in lost revenue, halted production lines, and compromised safety. Operational resilience now depends entirely on uncompromising cybersecurity.

A DATA-LED FIELD REPORT

## *1,020*

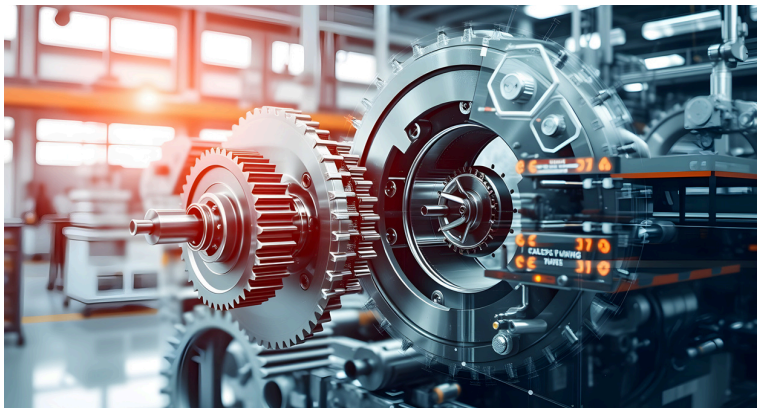
***industrial ransomware victims***

*observed in Q1 2026

Cyber threats have moved from theoretical risks to systemic operational disruptions. This figure is a stark indicator that attackers are actively targeting the industrial sector, making proactive defense a core business imperative.

There is a common misconception that an attacker must be a specialized genius capable of rewriting the code inside a robotic arm to cause a disaster. The 2026 research clarifies a much simpler reality: Ransomware does not need to "hack the PLC" to stop the line.

If an attacker disrupts the identity management systems or the virtualization servers hosting the MES, the factory floor goes dark. The machines haven't been "hacked," but they no longer have the instructions or authorization required to operate



## Key Insight:

Manufacturing remains the primary target of industrial cybercrime. In Q1 2026, **62% of all observed industrial victims (633 out of 1,020)** were in the manufacturing sector. These incidents highlight how "cascading" IT failures—standard ransomware hitting office systems—are now the leading cause of physical downtime.

## 62%

### *manufacturing*

**Enterprise IT disruption - identity, ERP, MES, virtualization and remote access -continues to cascade into OT withoutICS-specific malware.**

**3,300**
industrial victims
*2025*

**27.7%**
of IBM-observed incidents
*manufacturing*

## What is happening:

### 01 *Volume has reset upward*

- Dragos observed 605 industrial ransomware victims in 2022;
- 3,300 in 2025. Q1 2026 alone added 1,020.

### 02 *Impact crosses the boundary*

- Operational shutdown can begin in enterprise systems that schedule production, manage identity or host engineering workloads.

### 03 *The attacker advantage is basic*

- Public-facing exploitation, stolen credentials and weak third-party controls remain the dominant entry conditions.

## *Third-Party Exposure*

A massive 61% of breaches involve a vendor or supplier. This often manifests as Distributed Remote Access, where maintenance contractors have permanent "always-on" VPN tunnels into the factory. Attackers compromise the smaller vendor to walk straight into the larger manufacturer.

Attackers today are largely "financially motivated" professionals. They don't look for the most complex way in; they look for the most reliable. Research shows four primary entry points into the manufacturing environment:

- Vulnerability Exploitation (38%)
- Phishing (13%)
- Credential Abuse (11%) – This involves using stolen passwords.

**61%**
manufacturing breaches
*ransomware*

**30%**
of OT networks
*have visibility*


> *Ransomware does not need to "hack the PLC" to stop the line. Converged infrastructure makes IT availability part of process resilience. The most dangerous gap is often not exotic malware-it is uncertainty about what is connected, trusted and recoverable.*

# ARCHITECTING SAFETY INTO THE SYSTEM

The path of a modern attack is rarely a single "hack." It is a business process that flows from an Infostealer (malware designed to grab passwords) to the Credential Market (dark-web forums where hackers buy/sell those stolen logins), eventually leading to Enterprise Access, Data Theft, and Extortion.

Operational resilience is not about chasing "exotic" threats; it is about securing the ordinary systems—like identity and virtualization—that keep the line moving.

# GET IN TOUCH

JOWANZA@PARAKEETFINANCIAL.COM

PARAKEETRISK.COM