DENEXUS™

MAY 2026 | NEWSLETTER

OT CYBER RISK INTELLIGENCE NEWSLETTER

Thought Leadership · Industry Events · CEO Insights

15+
Threat Signals

5
Industry Events

3
Key Insights

01 The OT Cyber Insurance Gap
02 Industry Events & Threats
03 DeNexus Events
04 CEO Insights

denexus.io

CONTENTS

01 **The OT Cyber Insurance Gap**
Where recoverability is decided early
Page 3

02 **Industry Events & Threat Signals**
OT cyber attacks, threats & market updates
Page 5

03 **DeNexus Events**
Where you'll find us this month
Page 9

04 **CEO Insights**
The question no one asked
Page 11

Key Focus Areas

This month's newsletter covers critical updates on OT cyber insurance, emerging threat signals, and upcoming industry events where DeNexus will be present.

Thought Leadership

01

The OT Cyber Insurance Gap

Where Recoverability Is Decided Early

Cyber-physical loss often falls into seams between traditional coverages. The issue is structural: wordings, triggers, exclusions, waiting periods, and restoration definitions do not always align cleanly with OT loss mechanics.

The OT cyber insurance gap: where recoverability is decided early

Cyber-physical loss often falls into seams between traditional coverages. The issue is structural: wordings, triggers, exclusions, waiting periods, and restoration definitions do not always align cleanly with OT loss mechanics.

What matters this month

The gap is structural

Recoverability can hinge on definitions of cause, duration, and restoration.

Proof bundles reduce surprises

Underwriting and claims confidence improves when artifacts are standardized and current.

Insurability is earned

Confidence increases when controls demonstrably change feasible outcomes.

What you can do now

1. Build a loss-to-coverage mapping matrix (loss mechanism to evidence needed to likely policy touchpoints).
2. Prepare a facility dossier: access governance, segmentation reality, restore testing, and OT-ready incident response procedures.
3. Translate technical reality into a concise, defensible market narrative (bounded scenarios, explicit assumptions).

Next month: Underwriting-grade evidence: small, structured, defensible.

Industry Events & Threat Signals

02

OT Cyber Attacks, Threats & Market

What the industry is watching this month

Cyber-physical loss often falls into seams between traditional coverages. The issue is structural: wordings, triggers, exclusions, waiting periods, and restoration definitions do not always align cleanly with OT loss mechanics.

OT Cyber Attacks & Incidents

Stryker — Self-Insured. 5.0% Loss. $375M Floor.

Stryker deliberately chose to self-insure — a stated governance decision on its own corporate website. On March 11, Handala (MOIS-affiliated) weaponized Stryker's Microsoft Intune MDM platform using 278 stolen credentials to wipe ~40,000 devices across 79 countries. ECG transmission offline statewide in Maryland. Surgical delays at CommonSpirit Health. Q1: $6.0B vs. $6.34B expected — 5.0% of annual revenue lost in one quarter. RBC derived ~$375M total impact, all on Stryker's balance sheet. No policy, no recovery. That is the floor: rebuild costs, six-plus employee PII lawsuits, potential patient safety litigation, and the revenue tail from customer churn are not in the Q1 filing. Five analysts on the Q1 call. Not one asked whether the self-insurance decision was made with this threat in the risk model. Management volunteered nothing.

5.0%	-8.5%	-190bps	~3 weeks
Q1 Revenue Lost	Adjusted EPS	Gross Margin	Production Offline

Sources: Q1 2026 Earnings Press Release · Q1 2026 Earnings Call Transcript · Stryker Customer Update · Coalition Incident Analysis

Iranian-Linked Actors Targeting U.S. Infrastructure PLCs — CISA Joint Advisory

CISA, FBI, and NSA jointly confirmed that Iranian-linked actors have infiltrated programmable logic controllers at U.S. ports, power plants, and water facilities. Unit 42 documented a new cluster (CL-STA-1128) installing Rockwell Automation FactoryTalk on VPS infrastructure — capability development, not opportunistic scanning. The pre-positioned access has not been recalled. The advisory remains in effect.

U.S. Ports · Power Plants · Water Facilities

Source: CISA Advisory AA26-097A · Picus Security / Unit 42 Analysis

Threat Signals

FIRESTARTER Backdoor — Cisco ASA/Firepower

CISA and NCSC warned that FIRESTARTER malware establishes persistent backdoor access to Cisco firewall infrastructure and survives patching. Cisco ASA/Firepower devices sit at the IT/OT perimeter in many industrial environments — persistence after patching means segmentation assumptions based on remediation timelines are unreliable.

Sources: CISA Analysis Report AR26-113A · The Record

China-Nexus Covert Edge Networks — Five Eyes Advisory

A joint NSA/CISA/NCSC/international advisory documented China-linked actors using covert networks of compromised edge and IoT devices to obscure attribution and pre-position across critical infrastructure. For insurers: the same concealed access infrastructure enables simultaneous compromise across multiple policyholders with no visible common vector — a direct accumulation signal.

Sources: NSA Press Release · ASD/ACSC Executive Summary

Cyber Insurance Market

Resilience — Manufacturing Ransomware Data

Resilience's latest claims analysis shows manufacturing leads global cyberattack targets, with ransomware accounting for 90%+ of losses from just 12% of claims. The tail is short but severe — exactly the loss profile that soft-market pricing is least equipped to handle.

90%+

Ransomware Losses

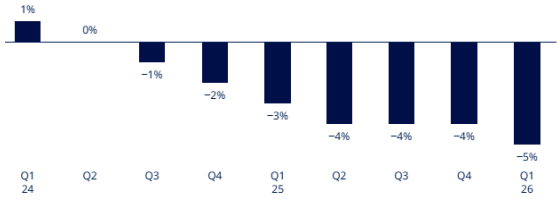
12%

Claims Generating Losses

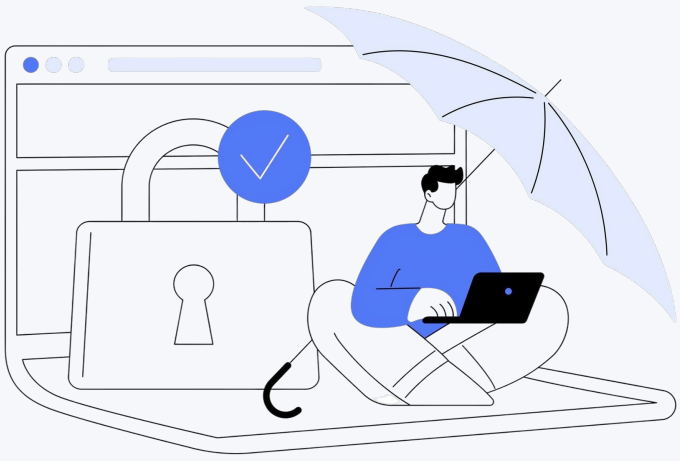
Sources: Resilience Claims Analysis — PR Newswire

Marsh Q1 2026 — Seventh Consecutive Rate Decline.

Marsh's Q1 Global Insurance Market Index recorded a 5% cyber rate decrease — the seventh consecutive quarterly drop. The window for industrial buyers to improve structure and limits before conditions harden is still open. Industrial operators with unquantified OT exposure are entering renewal in the most favorable pricing environment in three years — and may not see another one.



Sources: Marsh Global Insurance Market Index Q1 2026



DeNexus Events

03

Where You'll Find Us

May – June 2026

Join us at industry events where DeNexus experts will share insights on OT cyber risk, threat intelligence, and risk quantification.

5 Events | May 7 - June 16

Upcoming Events

7 MAY

Fortinet

Cybersecurity solutions and threat intelligence.
Presenting: **"Where Sound Risk Management Breaks on the Plant Floor"**

Jose Seara

1-3 JUN

Gartner Risk Summit

Enterprise risk management and governance

Jose Seara

8-10 JUN

SANS ICS Summit

Industrial control systems security.
Presenting: **"From Dwell Time to Dollars: Quantifying the Financial Value of Faster OT Incident Recovery "**

Donovan Tindill

9 JUN

Fortinet OT Summit

Operational technology security.
Presenting: **"The Cyber-Physical Balance Sheet: Managing OT Cyber Risk, Insurance, and Resilience"**

Donovan Tindill Virtual

16 JUN

OT ISA, Prague

ISA OT cybersecurity standards and practices.
Presenting: **"OT Cyber-Physical Risk Management"**

Jose Seara

CEO Insights

The Question No One Asked

Read Jose M. Seara's latest LinkedIn article:

Why OT Cyber Risk Quantification Matters More Than Ever

In the wake of recent high-profile attacks on critical infrastructure, organizations are realizing that traditional cybersecurity metrics fall short when it comes to operational technology. The disconnect between IT security teams and OT operations is creating blind spots that threat actors are actively exploiting...

May 4, 2026 | 5 min read | 1.2k views

Read on LinkedIn

 | www.denexus.io