Q3 2025 INCIDENT ANALYSIS

Industrial Cyber Risks

Key OT cyber incidents, insurance trends, and the case for industrial cyber risk quantification.

PUBLISHED BY

DENEXUS™

DATE

November 2025

OVERVIEW

Presentation Agenda

01

Q3 2025 Incident Landscape

Analysis of OT/industrial cyber incidents, trends, and impacted sectors.

02

Jaguar Land Rover Case Study

Analysis of the £882M total impact (incl. £485M direct revenue loss) and key lessons learned.

03

Ransomware & Hacktivist Trends

Data on surge in attacks targeting manufacturing and critical infrastructure.

04

Insurance Market & Gaps

Premium shifts, coverage limitations, and the growing protection gap.

05

Why Quantification Matters

Moving from qualitative checklists to financial risk metrics.

06

How DeNexus DeRISK™ Helps

Platform overview, capabilities, and client success outcomes.

EXECUTIVE SUMMARY

What Leaders Need to Know

Watershed Moment for OT: Q3 2025 saw industrial cyberattacks reach unprecedented scale and sophistication, moving beyond theoretical risks.

Major Incidents: The quarter was defined by the Jaguar Land Rover £882M total impact (£485M direct revenue loss) and a 26% surge in manufacturing ransomware.

Physical Consequences: OT sites experiencing cyber incidents with physical impacts jumped 146% YoY, proving that OT attacks are no longer low-impact events.

Insurance Paradox: Global premiums fell (-6%) due to capacity, yet underwriting rigor for quantification increased significantly.

Systemic Exposure: Modeled severe global OT cyber losses could reach $329.5B, highlighting the need for advanced risk modeling.

Sources:

- ITPro: JLR Incident Analysis
- Waterfall: 2025 OT Threat Report
- FERMA: Cyber Insurance Analysis
- GuidePoint: GRIT Q3 2025 Report
- Marsh: Insurance Market Index
- SecurityBrief: Global OT Loss Analysis

STRATEGIC IMPERATIVE

"Industrial cyber risk is no longer just an IT problem."

It has evolved into a board-level financial risk that requires quantified management, not just compliance checklists.

QUANTIFY

INSURE

PROTECT

Q3 2025 IMPACT ANALYSIS

By The Numbers

Key statistics revealing the escalation of industrial cyber risk.

HISTORICAL RECORD

£882M

($1.1 Billion USD)

Total JLR Impact

Costliest industrial cyberattack in history following a 6-week production shutdown.

Note: £485M represents direct revenue loss component only. See Slide 8 for complete breakdown of all impact categories.

INSURANCE MARKET

-6%

Global Premium Rate Change

Softening Market

POTENTIAL EXPOSURE

Modeled Global OT Losses

Under severe but plausible attack scenarios.

$329.5B

SEVERITY SURGE

+146%

OT Sites with Physical Consequences

↑ Year-Over-Year

FREQUENCY

252

Manufacturing Ransomware Incidents

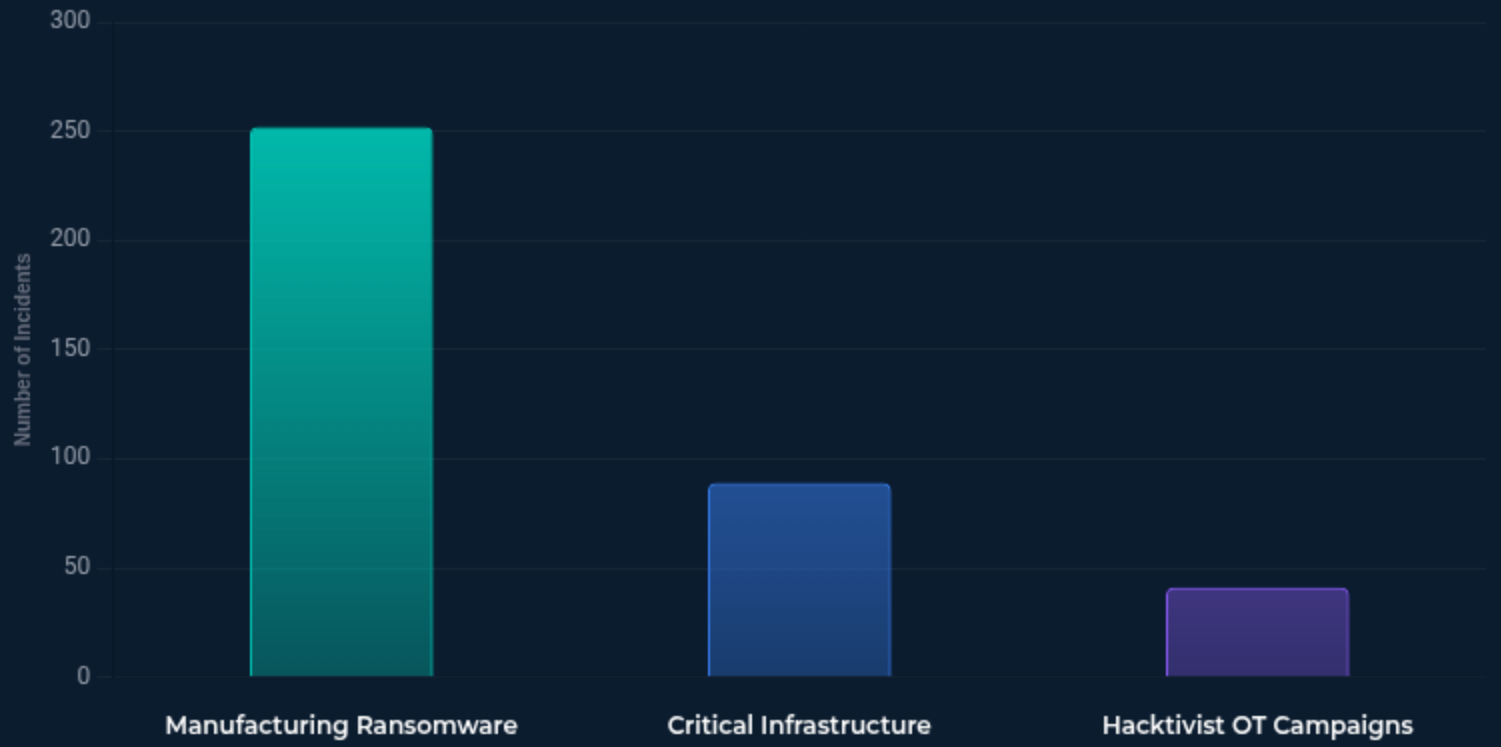
↑ 26% vs Q2

Sources: JLR Impact (ITPro) · Global OT Losses (SecurityBrief) · Physical Impact Data (Waterfall Security) · Ransomware Data (GuidePoint GRIT) · Premium Rate Data (Marsh)

INCIDENT ANALYSIS

Q3 2025 Incident Landscape

Escalating attack frequency across manufacturing and critical infrastructure sectors.



	Manufacturing Ransomware	Critical Infrastructure	Hacktivist OT Campaigns
CHANGE VS Q2	↑ 26%	↑ 18%	↑ 100%
YEAR-OVER-YEAR	+61%	+95%	+220%

KEY TAKEAWAY

OT attacks are becoming both more frequent and more consequential, with physical impacts accelerating faster than general incident rates.

Physical Impact Surge

OT SITES WITH PHYSICAL CONSEQUENCES

146% ↑YoY

Confirmed incidents with actual operational disruption

- Verified physical consequences
- Not potential vulnerabilities

SOURCES:

- GuidePoint Security GRIT Q3 2025 Report (Manufacturing Ransomware Data)
- Waterfall Security 2025 OT Threat Report (Physical Impact Data)
- Cyble (Hacktivist OT Campaign Data)

GLOBAL RISK QUANTIFICATION

The $329.5 Billion Question

Coordinated industrial OT attacks could drive catastrophic global losses under severe scenarios.

POTENTIAL GLOBAL EXPOSURE

$329.5B

Severe Scenario Modeling

Advanced risk modeling reveals that coordinated attacks on industrial infrastructure could generate losses exceeding $300B, challenging global insurance capacity.

PREVALENCE

22%

Organizations Hit Last Year

Experienced a confirmed OT cybersecurity incident.

CONSEQUENCE

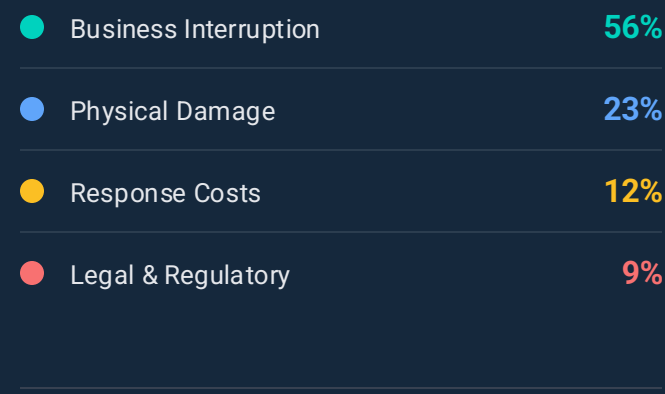
40%

Resulted in Disruption

Incidents leading to actual operational downtime.

LOSS DISTRIBUTION PREVIEW

Where the Cost Lies



"Business interruption is the primary driver, accounting for over half of potential losses."

Source: SecurityBrief: OT cyber incidents may cost up to USD 329.5 billion globally

CASE STUDY: JAGUAR LAND ROVER

Anatomy of a Disaster: Timeline

How a seemingly routine intrusion cascaded into a six-week production shutdown.

LATE AUGUST 2025

Network Intrusion

Attackers compromised IT network. They understood JLR's IT/OT integration and just-in-time production dependencies.

SEPT 1, 2025

Detection & Stop

Intrusion detected. IT systems shut down as precaution. Unexpected consequence: Manufacturing dependent on IT data halted immediately.

SEPT 1 - 30, 2025

Total Production Halt

Complete shutdown across all UK facilities. Highly automated lines could not operate without real-time data flows from compromised infrastructure.

⊘ ZERO OUTPUT

OCT 1 - 14, 2025

Phased Restart

Complex recovery process. Multiple setbacks occurred as system contamination and safe sequencing challenges emerged during restart.

⚠ Impact Reality Check

A single IT/OT dependency failure triggered a multi-week shutdown because the organization lacked quantified scenarios for safe manual operations.

Source: ITPro: JLR Cyber Attack Financial Impact Analysis

FINANCIAL ANALYSIS

JLR Financial Impact Breakdown

Integrated IT/OT dependencies turned a security incident into the costliest industrial cyberattack in history.

Cost Components

Direct Revenue Loss	£485M
Supply Chain Penalties	£127M
Recovery Costs	£89M
Supplier Support	£156M
Insurance Deductible	£25M

TOTAL IMPACT **£882M**

approx. $1.1 Billion USD

Losses accumulated over 6-week shutdown period

Values presented in GBP (£) millions.

Sources: ITPro JLR Incident Analysis

STRATEGIC TAKEAWAYS

Lessons for OT-Intensive Organizations

Critical gaps revealed by the JLR incident that every industrial leader must address.

1

IT/OT Integration Risk

Modern manufacturing's efficiency gains come with cascading failure risks that traditional security models fail to address. Just-in-time processes create fragile dependencies where IT failures immediately halt OT production.

2

Recovery Complexity

Restarting integrated industrial systems safely requires careful sequencing that can take weeks or months. Manual workarounds are often theoretical and fail under the pressure of a real-world cyber crisis.

3

Supply Chain Amplification

A single manufacturer's shutdown triggers billion-dollar ripple effects. Contractual penalties and supplier support costs can exceed direct revenue losses, amplifying the financial impact significantly.

4

Insurance Gaps

Even sophisticated cyber insurance policies may not cover the full scope of business interruption in highly integrated environments. Standard limits are often exhausted by the sheer scale of industrial downtime costs.

> *"The severity of the JLR incident could have been significantly reduced, if detected in the early attack stages, with proper risk quantification and scenario modeling."*

THREAT LANDSCAPE EVOLUTION

Ransomware & Hacktivist Trends in OT

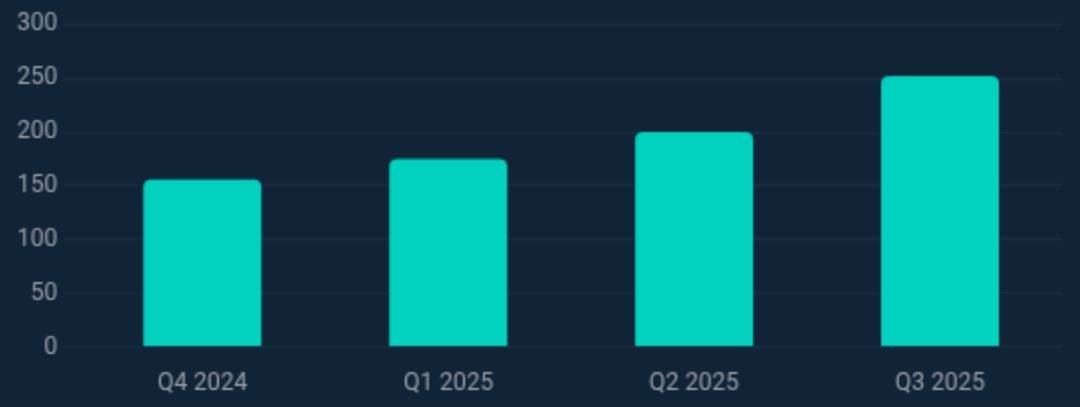
Dual surge in criminal extortion and politically motivated disruption targeting industrial assets.

Manufacturing Ransomware

252

INCIDENTS PER QUARTER

↑ 26% QoQ ↑ 61% YoY

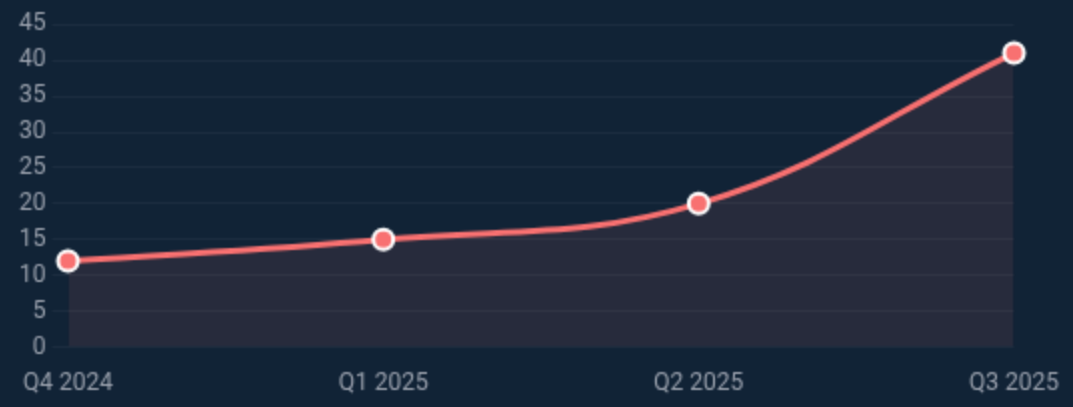


Hacktivist OT Campaigns

41

CAMPAIGNS PER QUARTER

↑ 100% QoQ ↑ 220% YoY



PREVALENCE

22%

Organizations experienced an OT incident in past year

IMPACT

40%

Incidents resulted in operational disruption

WHAT THIS MEANS FOR OT LEADERS

Attackers are aggressively pivoting from IT to OT environments. Security strategies must prioritize preventing lateral movement and securing supply chain intrusion paths rather than just perimeter defense.

SOURCES: Ransomware Data: GuidePoint Security GRIT Q3 2025 Report | Hacktivist Campaigns: Cyble: Hacktivist Attacks on Critical Infrastructure Q3 2025

MARKET ANALYSIS

Insurance Market Shifts: The Great Recalibration

While premiums soften globally, underwriting standards are becoming increasingly rigorous.

REGION	RATE CHANGE	MARKET CONDITION	CAPACITY TREND	PRIMARY DRIVER
Global Average	- 6%	Soft	↑ Increasing	New carrier capacity entering market
Europe	- 12% to -15%	Very Soft	Abundant	Intense competition for market share
North America	- 2% to -6%	Soft	= Stable/Increasing	Improved risk controls adoption
Asia-Pacific	- 4% to -8%	Soft	Growing	Market development & maturity

THE UNDERWRITING EVOLUTION

Quantified Risk Models
Shift from checklists to financial impact modeling

OT-Specific Coverage
Tailored forms for operational technology risks

Dynamic Pricing
Premium adjustments based on real-time controls

> *"Clients with demonstrated stronger security controls achieved 20-25% greater rate reductions in Q3 2025, clearly showing that evidence-based risk management drives both security and economic outcomes."*
>
> — FERMA CYBER INSURANCE REPORT

Sources:
Rate Changes: Marsh Global Insurance Market Index
Controls Impact: FERMA Demystifying Cyber Insurance Report

GLOBAL LOSS MODELING

Severe Scenario Impact Analysis

Breakdown of potential $329.5 billion global losses under coordinated OT attack scenarios.

LOSS COMPONENT BREAKDOWN

Business Interruption $184.5 Billion	56%
Physical Damage $75.8 Billion	23%
Response Costs $39.5 Billion	12%
Legal & Regulatory $29.7 Billion	9%

DOMINANT RISK FACTOR

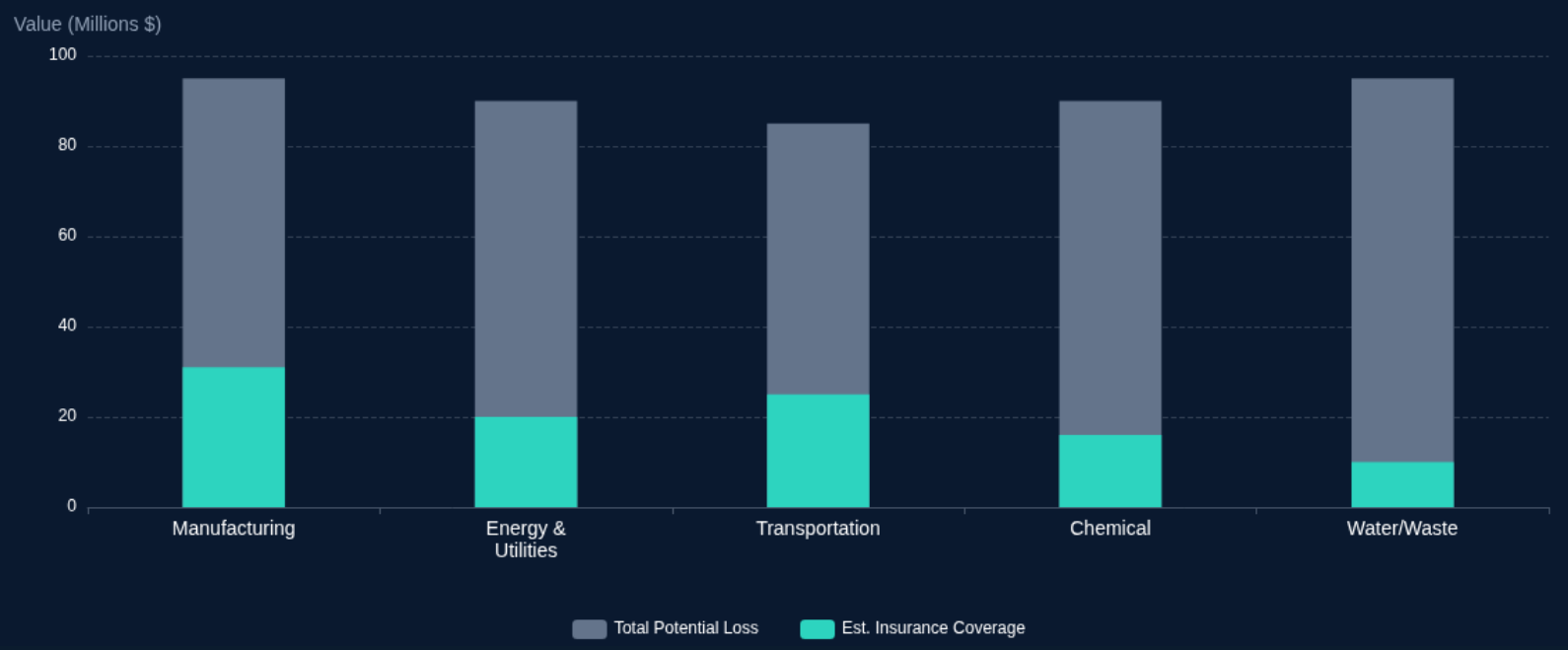
Business Interruption outweighs physical damage by more than 2x, confirming that operational downtime is the primary financial driver in systemic OT events.

Source: SecurityBrief: OT Cyber Incidents Global Impact Analysis

SECTOR ANALYSIS

Sector Vulnerability & Protection Gap

Massive disparity between potential OT losses and available insurance capacity across critical industries.



The Exposure Reality

Most industrial sectors are dangerously under-insured against catastrophic OT events. The average protection gap ranges from 67% to 89%.

Avg. Coverage	Avg. Gap
~28%	~72%

WHY THE GAP EXISTS

- Insufficient policy limits for catastrophic scenarios
- Exclusions for nation-state & systemic attacks

Coverage confusion: Physical damage from cyber events often falls between policy types — cyber insurers may consider it property damage while property insurers view it as cyber-excluded

Data Source: Dragos & Marsh McLennan, 2025 OT Security Financial Risk Report

Sources: Munich Re Cyber Insurance Risks & Trends 2025

METHODOLOGY SHIFT

Why Quantification Matters

Moving from subjective checklists to financial certainty is critical for modern industrial risk management.

Traditional Approach

QUALITATIVE & COMPLIANCE-BASED

- Reliant on compliance checklists and maturity scores that don't map to risk.
- Subjective "Red/Amber/Green" heatmaps that lack precision.
- Limited visibility for Boards into actual financial exposure.
- Difficult to optimize insurance coverage or justify ROI.

"Are we compliant?"

VS

RECOMMENDED

Quantified Approach

FINANCIAL & DATA-DRIVEN

- Calculates Value-at-Risk (VaR) and Expected Annual Loss (EAL).
- Uses probabilistic scenario modeling based on real OT data.
- Empowers ROI-based investment prioritization.
- Directly translates cyber risk into business financial terms.

"How much will we lose, and how do we stop it?"

RISK REDUCTION

18.5%

Average risk reduction from implementing incident response planning

CONTROL EFFECTIVENESS

17%

Risk reduction from defensible architecture implementation

VISIBILITY IMPACT

16.5%

Risk reduction from ICS network visibility & monitoring

Source: Dragos & Marsh McLennan Cyber Risk Intelligence Center (CRIC), 2025 OT Security Financial Risk Report

SCIENTIFIC RISK MANAGEMENT

DeRISK™: Comprehensive OT Cyber Risk Quantification

The industry's leading platform empowering organizations to identify, quantify, and manage cyber risk exposure across industrial environments using data-driven financial metrics.

Cyber Risk Quantification (CRQ)

Translate technical signals into financial exposure metrics.

- Value-at-Risk (VaR)
- Expected Annual Loss (EAL)
- Return on Mitigation

Quantified Vulnerability Mgmt

Prioritize remediation based on financial impact, not just CVSS scores.

- Risk-Based Prioritization
- Asset Criticality Mapping
- Mitigation ROI

Scenario Modeling

Simulate sophisticated OT attacks to understand potential impacts.

- Monte Carlo Simulations
- Ransomware & Sabotage
- Equipment Damage

Insurance Optimization

Align coverage with actual exposure and negotiate better terms.

- Coverage Gap Analysis
- Premium Negotiation
- Limit Adequacy Check

KEY OUTCOMES:

- **Financial Certainty** — Defensible metrics for the Board
- **Actionable Intelligence** — Clear roadmap for risk reduction
- **Efficient Transfer** — Optimized cyber insurance portfolio

PROCESS ARCHITECTURE

How DeRISK™ Works in OT Environments

End-to-end quantification workflow transforming technical data into financial intelligence.

01 INPUT
Data Ingestion

- OT Asset DiscoveryAutomated inventory & mapping
- Network TopologySegmentation & flow analysis
- Dependency ModelingIT/OT interdependency mapping

02 ANALYSIS
Risk Modeling

- Vulnerability Assessment Context-aware threat scoring
- Threat Intelligence Real-time actor profiling
- Monte Carlo Simulations Probabilistic loss forecasting

03 OUTCOME
Actionable Outputs

- Financial MetricsEAL & Value-at-Risk (VaR)
- Prioritized ActionsROI-based mitigation plans
- Insurance Gap AnalysisCoverage optimization data

Continuous Monitoring: Platform dynamically updates risk models as asset states and threat landscapes evolve.

TAKE ACTION

What's Next?

Transform your industrial cyber risk management from reactive to proactive with DeNexus.

Request Assessment

Request a DeRISK™ assessment of your OT environment to establish a defensible risk baseline.

Align Strategy

Align OT cyber risk with your insurance strategy to optimize coverage and reduce premiums.

Schedule Workshop

Schedule a private workshop with DeNexus risk experts to customize your roadmap.

Start Your Transformation →

www.denexus.io **info@denexus.io**