DENEXUS

BUYER'S GUIDE

INDUSTRIAL CYBER RISK · FOR RISK MANAGERS & LEADERSHIP

From Invisible to Manageable: A Practical Guide to OT Cyber Risk

How industrial organizations translate OT cyber exposure into financial decisions — and what it takes to quantify, reduce, and transfer risk with evidence at every step.

300+
INDUSTRIAL DEPLOYMENTS
US & EU

4
OT SECTORS COVERED
POWER · T&D · MFG · DC

3
MOVES IN THE
OPERATING MODEL

SECTION 1

OT Cyber Risk Has No Natural Financial Unit

Most industrial organizations know they have OT cyber exposure. Almost none can say what it costs.

The gap is not in detection. Most organizations have visibility into their OT environment — they can see the assets, the vulnerabilities, the network topology. The gap is in translation: the step between technical risk and financial risk that makes OT exposure legible to governance, finance, and the insurance market.

> If an OT incident shut down your largest facility today, how quickly could you give the CFO a credible financial estimate? Not a severity rating — an actual number: expected loss per day, estimated restoration duration, tail scenario with bounded assumptions.

For most industrial organizations, the answer is either "I can't" or "weeks." That gap is the problem this guide addresses.

WHY TRADITIONAL APPROACHES FALL SHORT

VULNERABILITY SCORES

CVSS ranks data integrity risk — not process consequence

A CVSS 9.8 vulnerability in an air-gapped segment with compensating controls may have near-zero financial exposure. A CVSS 5.2 on a critical process path with no segmentation may drive six-figure loss. The score does not tell you which is which.

QUALITATIVE ASSESSMENTS

Narrative risk does not translate to capital decisions

Consultancy reports, red team findings, and heat maps give leadership a story. Stories cannot size insurance programs, justify security budget to a CFO, or satisfy a board's duty of oversight. A defensible number requires a traceable methodology.

MATURITY FRAMEWORKS

Posture assessments do not produce financial decisions

A maturity score tells you where you sit relative to a framework. It does not tell you what exposure you carry, which investments move the loss curve, or what premium a market will charge. Governance and finance teams cannot act on a percentile.

INCIDENT RESPONSE PLANS

Knowing what to do is not the same as knowing what it costs

A well-prepared IRP improves recovery speed. It does not quantify pre-incident exposure, model tail scenarios, or produce the evidence an underwriter needs to price the risk. Preparation and quantification are different disciplines.

SECTION 2

Quantify. Reduce. Transfer. The Three-Move Operating Model

Each move in the operating model produces a specific output for a specific audience. Together they close the gap between OT technical risk and financial risk management.

01 QUANTIFY

Product: DeRISK™ CRQ

Translate OT cyber exposure into a financial risk currency — Annual Expected Loss and Value at Risk, built bottom-up from your specific OT environment. The quantification output is the shared language that engineers, executives, and markets can all act on. It is not a score, not a tier, and not a narrative. It is a number with a traceable evidence chain and bounded assumptions.

Produces: AEL · VaR · Loss Exceedance Curves · Ranked Action Points · Governance Artifact

02 REDUCE

Products: DeRISK™ CRQ + DeRISK™ QVM

Prioritize security investments by what moves the loss curve — not by what scores worst on a severity ranking. Every vulnerability in your environment receives a dollar value: the expected loss reduction if that CVE is remediated. The remediation sequence is constraint-aware: ordered within your actual operational windows, vendor dependencies, and staffing limits. What you get is not a plan that looks right on paper. It is a plan that executes.

Produces: Dollar per CVE · Loss-Ranked Remediation · ROI per Security Investment · Framework Output

03 TRANSFER

Product: DeRISK™ UWA Agentic

Convert your risk posture into a structured market submission. Five specialist AI agents process OT cyber submissions to full actuarial output — expected loss, loss exceedance curves, premium indication, a structured insurance program, and binding conditions with deadlines — in 10 to 20 minutes. The evidence you built in the Quantify and Reduce steps becomes the input that earns capacity and drives better placement terms.

Produces: EL · MFL · Premium Indication · Structured Insurance Program · Binding Conditions

> The three moves are not sequential milestones. They are a continuous operating model. Organizations that run them in parallel — always quantifying, always reducing, always maintaining transfer-ready evidence — compound credibility over time. The market rewards the compounding programs because the evidence quality is visible.

SECTION 3

The Three Tests a Risk Number Has to Pass

A risk quantification output is only as useful as its defensibility. These are the three tests that separate a governance asset from a document.

1. **A CFO can understand the key assumptions without a technical briefing.**
   The output must be explainable in plain financial language: these scenarios, these assumptions, this evidence, this number. When the CFO asks "why this number?" the answer must be traceable without requiring an interpreter. If the methodology requires a specialist to explain it, it will not earn governance confidence.

2. **An underwriter can trace the loss estimate back to specific facility evidence.**
   Narrative submissions cannot be compared, aggregated, or governed. A structured loss estimate with traceable assumptions — facility data, model version, bounded scenarios — is the input that markets can price with confidence. When renewal comes, the question is not "what's changed?" It is "here is what changed, and here is how the curve moved."

3. **An operator can follow the logic from their facility to the output — and change it.**
   A black-box number is not defensible. A number that traces from network access event to process disruption to recovery economics — at the specific facility, with the specific architecture — can be challenged constructively, updated when conditions change, and relied upon across decision contexts.

HOW THE URMS ENGINE PRODUCES THIS OUTPUT

300+	4	AEL	Full
DEPLOYMENTS	**OT SECTORS**	**PRIMARY OUTPUT**	**AUDIT TRAIL**
Calibration basis — US & EU industrial facilities	Power · T&D · Manufacturing · Data Centers	Annual Expected Loss — facility-level, portfolio-level	Every output traceable to source inputs and model version

DeRISK CRQ models the path from network access event to process disruption to recovery economics — facility by facility, scenario by scenario. It does not start from threat scores. It starts from process consequence and works backward to the access conditions that could produce it.

The output — Annual Expected Loss, Value at Risk, and loss exceedance curves — is not an opinion. It is a governed artifact: versioned, traceable, and updatable as architecture, controls, or threat conditions change.

> **A number nobody can explain is a liability dressed as analysis.** An explainable number with an audit trail is a governance asset — one that can be challenged, updated, presented to markets, and defended in a claims context.

SECTION 4

What Changes When OT Risk Gets a Financial Number

The shift is not just analytical. It changes the conversations that matter most — with the board, the CFO, the insurance market, and the security team.

BOARD & AUDIT COMMITTEE

From qualitative briefing to governance artifact

AEL and VaR on the board dashboard update as exposure changes. Directors fulfill their duty of oversight with a number that can be challenged and explained — not a heat map that cannot be acted on.

CHIEF RISK OFFICER

From evidence gap to transfer-ready submission

The Chief Risk Officer sits at the intersection of both worlds. CRQ evidence in. UWA actuarial output out. The same quantification that governs internally becomes the structured submission that earns capacity externally.

CFO & FINANCE

From narrative to balance sheet line

Expected loss reduction per dollar of remediation spend. VaR as a quantified balance sheet exposure. Insurance spend justified by modeled loss, not benchmarks. Every budget conversation changes when the CISO speaks CFO language.

INSURANCE MARKET

From narrative to priceable exposure

Structured submissions with bounded scenarios and traceable assumptions produce better placement outcomes. Underwriters can price with confidence. Binding conditions are explicit and trackable. Claims disputes are reduced by evidence built before the incident.

CISO & SECURITY TEAM

From severity scores to loss-ranked priorities

Which CVEs are actually driving financial exposure at which facilities. Which remediation actions move the loss curve most within real operational constraints. The security team stops defending a budget and starts managing a risk number.

COO & OPERATIONS

From IT security projects to operational risk management

Continuity scenarios grounded in facility-specific recovery economics. Remediation sequenced within maintenance windows and operational constraints. OT cyber risk managed as part of the enterprise risk register — not as a parallel security program.

SECTION 5

From the Field — What Customers Say Changes

Industrial operators and energy companies across power generation and manufacturing — what consistently shifts is the governance conversation.

> *The DeNexus software acts as a bridge between the cybersecurity team and the executive leadership group, as it allows me to quantify cyber risk with defendable metrics and ROIs.*

Jonathan Alexander
Director Cybersecurity · EDF

> *The DeRISK platform provides actionable data and reporting that helps us identify and communicate cybersecurity risks to the organization. It is a core component of our risk assessment, quantification, and remediation efforts.*

Scott Hooper
Director Cybersecurity · Clearway Energy

> *With DeRISK we understand our cybersecurity posture and can prioritize risk reduction and mitigation actions based on actionable financial data.*

Ken Young
CEO · Apex Clean Energy

> *DeNexus's risk quantification solution provides a granular cyber risk assessment of our company's OT environment.*

John Franzino
CEO · GridSecurity

300+	4	1
CRQ DEPLOYMENTS	**APPROVED QUOTES**	**PATTERN**
US & EU · Power, T&D, Manufacturing, Data Centers	Named customers · Attributed outcomes	Governance conversation changes when risk gets a dollar number

SECTION 6

Three Questions to Answer Before a Demo

The organizations that get the most from a first conversation with DeNexus come prepared with facility context. These three questions frame it.

1. **Which facilities drive your tail exposure?**
   Not which facilities have the most vulnerabilities — which ones, if disrupted, produce the most material operational and financial consequence. A manufacturing line with a 72-hour restart dependency is a different risk conversation than a monitoring system with a 2-hour failover. The quantification starts with process consequence, not CVE counts.

2. **What evidence exists for your current controls?**
   Documented controls and tested controls are not the same thing. A segmentation architecture that has not been validated against actual traffic patterns is an assertion, not evidence. Before a quantification produces defensible output, it needs to know which controls are tested, which are current, and which are attested but unverified. The gap between those categories is where pricing friction and claims disputes live.

3. **Is OT cyber risk in your governance framework — or your security program?**
   These are different programs with different audiences and different success metrics. Security programs manage controls. Governance programs manage risk — in financial terms, with board visibility and CFO-level accountability. The transition from one to the other is where quantification becomes necessary, and where the operating model in this guide becomes the right framework.

WHAT A FIRST CONVERSATION WITH DENEXUS COVERS

- → Your top 2–3 facilities and their consequence profiles
- → A preliminary AEL estimate from available data
- → Which OT visibility connectors are already in place
- → Current insurance program and renewal timeline
- → Which governance audience needs to act on the output
- → Where the evidence gaps are and how to close them

Ready to put a number on your OT cyber risk?

A 30-minute conversation is enough to produce a preliminary AEL estimate for your highest-consequence facility. No commitment. No sales pitch in the first session.

Book a conversation → denexus.io/contact

info@denexus.io · denexus.io · SOC 2 Type II Certified