CASE STUDY

Better Together:

Continuous Cyber Risk Quantification Meets OT Visibility

How a leading manufacturing company turned OT visibility into quantified financial risk across 2 industrial facilities — and proved which security investments reduce loss.

DeNexus

DeRISK CRQ — Cyber Risk Quantification for Industrial Enterprises

CUSTOMER PROFILE

A Leading Manufacturing Company

2	150+	Manufacturing
Facilities in Scope	Global Facilities	Sector
EU and Americas	Full portfolio	Discrete & Process

2 manufacturing facilities from a leading manufacturing company with 150+ industrial facilities worldwide. OT IDS was deployed at one facility for OT visibility. The next step: translating that technical visibility into business-level risk quantification the board and risk committee could act on.

THE CHALLENGE

Your OT platform tells you what's on your network. But who tells your board what it costs?

Vulnerability ≠ Financial Risk
Security teams reported CVE counts but could not express exposure in dollars — the language CFOs and boards understand.

No Cross-Facility Comparison
Two manufacturing plants in different regions operated without a common risk metric to drive capital allocation.

OT IDS Impact Unquantified
An OT IDS was deployed for visibility but no one could answer: did it change the risk picture? By how much?

No ROI for Mitigation Spend
Proposed security projects competed for budget with no way to rank them by risk reduction per dollar.

Communication Gap
The Risk Committee needed financial terms — dollars, confidence intervals — not CVSS scores or CVE counts.

Regulatory frameworks (NIS 2, IEC 62443) added urgency — but proactive risk management, not compliance, was the primary driver.

THE SOLUTION

DeRISK CRQ + Your OT Visibility Platform

Your OT Visibility Platform provides deep OT visibility — assets, vulnerabilities, network behavior. DeRISK CRQ takes that visibility and translates it into quantified financial risk. Together, they close the loop: see the environment, quantify its risk in dollars, prioritize what to fix, and prove the ROI.

OT Platform Provides	What It Captures	What DeRISK CRQ Does With It
Asset Inventory	OT devices, protocols, connections	Ingests asset data to build facility-specific risk models
Vulnerability Detection	CVEs, misconfigurations	Translates vulnerabilities into quantified financial exposure
Network Behavior	Traffic patterns, anomalies	Calibrates attack probability models with real telemetry

What DeRISK CRQ Delivers

Annual Expected Loss (EL)

The most probable annual cyber loss, in dollars. Answers the question every CFO asks: "What should we budget for?" Provides the baseline for cybersecurity investment planning, insurance coverage sizing, and cash reserve allocation. EL makes cyber risk comparable to every other operational risk the business already manages.

Value at Risk (VaR) — 95th & 99th Percentile

VaR quantifies the worst-case loss at a given confidence level. VaR 95th = maximum annual loss expected once every 20 years. VaR 99th = once every 100 years. Together they define the risk envelope: how bad could it get, and how much capital should the company hold in reserve? VaR drives board-level decisions on risk appetite, insurance limits, and catastrophic scenario planning.

Additional Capabilities

- **Portfolio Aggregation**
  Roll up facility risk to region or enterprise level
- **Loss Event Breakdown**
  Productivity loss, downtime, extortion, reputational damage
- **Pre- vs. Post-Telemetry**
  Prove the financial value of OT IDS deployment in dollars
- **Attack Vector Decomposition**
  Which MITRE ATT&CK techniques drive the most financial risk
- **Mitigation Simulation**
  Forecast risk reduction and ROI of proposed security investments
- **Continuous & Self-Adaptive**
  Risk model updates as the threat landscape evolves

Your OT Visibility Platform
Continuous OT asset discovery, vulnerability detection, and network behavior monitoring. Sees what is on the network and what threatens it.

+

DeRISK CRQ
Translates OT visibility into financial risk: Expected Loss, Value at Risk, attack vector decomposition, and mitigation ROI.

=

Together
The full loop: see it, quantify it in dollars, prioritize what to fix, prove the ROI.

Visibility alone doesn't reduce risk. Quantification alone can't see the network. You need both.

ENGAGEMENT SCOPE

Scope & Success Criteria

The engagement covered 2 manufacturing facilities across 2 regions (EU and Americas), with one facility running an OT IDS and one not yet deployed.

1. Quantify annual cyber risk for both manufacturing facilities
2. Ingest OT telemetry and measure its impact on risk quantification
3. Compare Pre-OT telemetry vs. Post-OT telemetry results for Plant A (EU)
4. Compare risk between the two facilities and regions
5. Simulate a risk mitigation project and quantify risk reduction
6. Identify top attack vectors and loss events for each facility
7. Deliver results in financial terms usable by the Risk Committee and Board

All 7 Criteria Achieved

RESULTS

The OT Telemetry Effect: Pre- vs. Post-Telemetry

After OT telemetry was ingested, portfolio risk went up — and that's the point. Previously invisible vulnerabilities surfaced, and DeRISK CRQ translated them into precise financial deltas. Without CRQ, the company would have seen more alerts but not known what they meant for the bottom line.

Metric	Pre-OT telemetry (Plant A)	Post-OT telemetry (Plant A)	Delta
Annual Expected Loss	~$600-625K	~$4.8-5M	+~700%
VaR (95th Percentile)	~$95-100K	~$29-30M	+>30,000%
VaR (99th Percentile)	~$7.9-8.1M	~$76-77M	+~855%

Key Insight:
More OT telemetry > more discovered vulnerabilities > higher (more accurate) risk quantification. The VaR 99th jumped from ~$8M to ~$76-77M — reflecting exposure that was always there, just not yet visible.

RESULTS

Facility Risk Comparison: Plant A vs. Plant B

PLANT A — EU | OT TELEMETRY ACTIVE

Annual Expected Loss

~$4.8–5M

+~700% vs. pre-telemetry

VaR (95th Percentile)

~$29–30M

VaR (99th Percentile)

~$76–77M

Control Maturity

~50%+ of controls at Repeatable / Adaptive level

Least mature: DETECT, RESPOND

OT Telemetry: Your OT Visibility Platform deployed

Your OT Visibility Platform deployment revealed significant hidden exposure. Risk picture increased sharply — reflecting a more accurate model, not new attacks.

PLANT B — AMERICAS | NO TELEMETRY

Annual Expected Loss

~$575–600K

Without OT telemetry — model less granular

VaR (95th Percentile)

~$2.4–2.6M

VaR (99th Percentile)

~$15–15.5M

Control Maturity

~73%+ of controls at Repeatable / Adaptive level

Least mature: IDENTIFY, PROTECT

OT Telemetry: OT IDS not yet deployed

Without OT telemetry, the risk model is less granular. Completing OT IDS deployment here is expected to surface additional exposure.

Takeaway:

Plant A (EU) carries ~8x the EL of Plant B (Americas) despite ~47% lower revenue. The difference is OT telemetry. Without OT telemetry, Plant B's risk model cannot yet see the vulnerabilities that telemetry would reveal. Your OT Visibility Platform deployment at Plant B is the highest-priority next step.

RESULTS

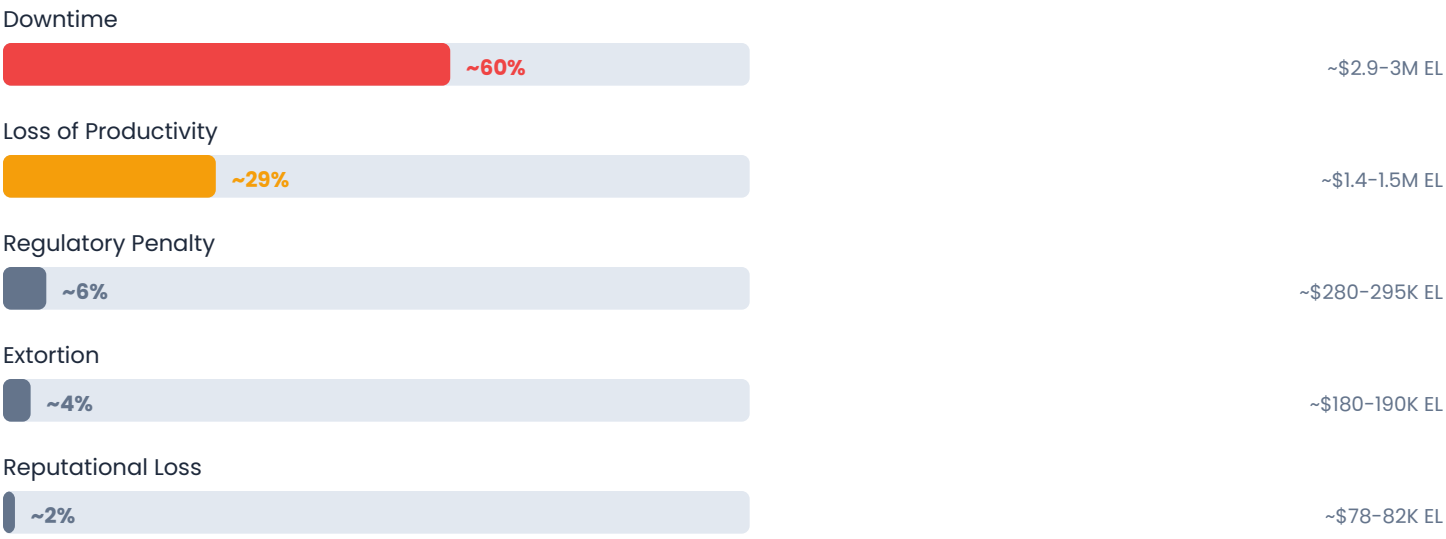
Drivers of Cyber Risk

DeRISK CRQ maps OT telemetry to MITRE ATT\&CK techniques and quantifies which attack paths and loss events carry the most financial risk — enabling security teams to allocate resources where they matter most. (Data: Plant A, EU facility)

Top Initial Access Vectors (MITRE ATT&CK mapped)

Remote service exploitation accounts for >60% of total expected loss. Phishing — ofte
n the focus of training budgets — ranks 3rd. DeRISK CRQ redirects investment to the vectors that actually drive loss.

Top Loss Events (Plant A)



Downtime + Productivity loss = ~89% of expected annual loss. Equipment damage — often assumed to be the worst case — is not in the top 5. CRQ realigns investment priorities to where loss actually occurs.

RESULTS

Mitigation ROI Simulation

DeRISK CRQ's Project Simulator quantified the risk reduction of a security investment project at Plant B (Americas) in dollars — enabling an evidence-based business case that no qualitative framework can provide. Each project's impact was expressed as dollar reductions in EL and VaR, not percent maturity improvements.

Project: Network Security Monitoring & IR Optimization 22 Controls | 102 Days | Target: Adaptive Maturity

~$38.5K	~$277.5K	~$263K
~8% reduction	~27% reduction	~2% reduction
Expected Loss Reduction	VaR 95th Reduction	VaR 99th Reduction

Pre- vs. Post-Implementation: Plant B (Americas)

Metric	Pre-Project	Post-Project	Reduction
Annual Expected Loss	~$460K	~$420K	~$38.5K (-8%)
VaR (95th Percentile)	~$1M	~$725K	~$277.5K (-27%)
VaR (99th Percentile)	~$12.9M	~$12.6M	~$263K (-2%)

Key Insight

Network Security Monitoring & IR Optimization is a high-value project with measurable EL and VaR reductions achievable in 102 days across 22 controls.

Without DeRISK CRQ's financial quantification, this project would compete for budget on technical merit alone — with no evidence of its dollar impact on risk exposure. CRQ gives security teams the business case they need to win budget.

Control Maturity Context

Plant A (EU)
~50%+ Repeatable / Adaptive
DETECT, RESPOND least mature
Less mature overall — telemetry active

Plant B (Americas)
~73%+ Repeatable / Adaptive
IDENTIFY, PROTECT least mature
More mature overall — telemetry not yet deployed

THE BIGGER PICTURE

From 2 Facilities to a Full Global Portfolio

"If 2 facilities carry combined portfolio VaR of ~$76-78M, what does the full portfolio look like?"

2
Facilities Assessed

»

Full Manufacturing Portfolio

This engagement assessed 2 of a multi-facility global manufacturing portfolio. Extrapolation to the full portfolio suggests enterprise-wide Value at Risk could be substantially higher than the engagement scope alone. This is not a prediction — it's a reason to scale. The engagement proved the methodology; full deployment provides the enterprise number.

OUTCOME

Three-Pronged Risk Strategy

Mitigate

Use CRQ to continuously evaluate risk exposure and simulate mitigation strategies with quantified ROI.

Transfer

Use CRQ outputs to optimize cyber insurance coverage and negotiate with brokers using data-backed risk figures.

Accept

For risks below threshold, quantify the acceptance level in dollar terms rather than relying on qualitative judgment.

Operational Next Steps

- Complete OT IDS deployment across remaining facilities to close the telemetry gap
- Expand DeRISK CRQ from 2-facility scope to full global manufacturing portfolio
- Adopt periodic CRQ cycles for all business entities and regions
- Use Project Simulator for ongoing mitigation planning and budget justification

REFERENCE

Glossary of Terms & Acronyms

Acronym	Full Term	Definition
AEL	Annual Expected Loss	See EL. Used interchangeably with Expected Loss in some contexts.
BCP	Business Continuity Plan	A documented strategy ensuring critical business functions continue during and after a disruption.
CMP	Crisis Management Plan	A framework for organizational response to a significant incident, covering communication, escalation, and decision authority.
CRQ	Cyber Risk Quantification	The process of expressing cyber risk in financial terms (dollars), enabling comparison with other business risks.
DRP	Disaster Recovery Plan	Technical procedures for restoring IT/OT systems and data after an incident.
EL	Expected Loss	The most probable annual cyber loss, in dollars. Represents the mean of the loss distribution — the amount a company should expect to lose on average each year. Used for budgeting, insurance sizing, and baseline risk communication.
IDS	Intrusion Detection System	A network security tool that monitors traffic for suspicious activity and known threats. In OT contexts, provides asset inventory and vulnerability detection.
MITRE ATT&CK	Adversarial Tactics, Techniques & Common Knowledge	A globally recognized knowledge base of adversary behaviors, used to classify and prioritize attack vectors by their real-world prevalence and impact.
OT	Operational Technology	Hardware and software that monitors and controls physical processes, equipment, and infrastructure (e.g., SCADA, PLCs, DCS).
VaR	Value at Risk	The maximum annual loss expected at a given confidence level. VaR 95th = worst case expected once every 20 years. VaR 99th = once every 100 years. Used for risk appetite setting, capital reserves, and catastrophic scenario planning.
VaR 95th	Value at Risk, 95th Percentile	Maximum loss expected with 95% confidence (1-in-20 year event). Informs insurance coverage and risk transfer decisions.
VaR 99th	Value at Risk, 99th Percentile	Maximum loss expected with 99% confidence (1-in-100 year event). Drives board-level capital allocation and worst-case planning.

In one engagement, 2 facilities worth of OT data became a quantified risk picture that reached the boardroom — and a prioritized investment roadmap backed by dollar figures, not gut feel.

Ready to quantify your OT cyber risk?

denexus.io

DeNexus

DeRISK CRQ — Cyber Risk Quantification for Industrial Enterprises