CASE STUDY

Better Together:

Continuous Cyber Risk Quantification Meets OT Visibility

How a leading European energy company turned OT IDS visibility into quantified financial risk across 16 industrial facilities — and proved which security investments actually reduce loss.

DENEXUS

DeRISK CRQ

CUSTOMER PROFILE

A Leading European Energy Company

3 Continents
EU, Americas, Asia-Pacific

16 Facilities
Wind, Solar, Combined Cycle

~3,300 MW
Total Generation Capacity

The company had deployed an OT IDS across a portion of its OT portfolio to gain visibility into assets and vulnerabilities. The next step: translating that technical visibility into business-level risk quantification that the board and risk committee could act on.

THE CHALLENGE

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

- **Vulnerability ≠ Financial Risk**
  Security teams reported CVE counts but couldn't express exposure in dollars — the language the CFO and Board understand.
- **No Cross-Portfolio Comparison**
  Different regions, technologies, and business units operated without a common risk metric.
- **IDS Impact Unquantified**
  An OT IDS was deployed, but nobody could answer: did it change the risk picture? By how much?
- **No ROI for Mitigation Spend**
  Six 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.

Regulatory frameworks (NIS 2, NERC CIP) 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 insight — 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. EL answers the question every CFO asks: "What should we budget for?" It provides the baseline for cybersecurity investment planning, insurance coverage sizing, and cash reserve allocation. EL is the metric that 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 represents the 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.

- **Portfolio Aggregation**
  Roll up facility risk to region, business unit, or enterprise level
- **Loss Event Breakdown**
  Productivity loss, downtime, reputational damage, extortion
- **Pre- vs. Post-Telemetry**
  Prove the financial value of IDS deployment
- **Attack Vector Decomposition**
  Which MITRE ATT&CK techniques drive the most financial risk
- **Mitigation Simulation**
  Forecast risk reduction and ROI of proposed security investments

The "Better Together" Thesis

Your OT Platform
Visibility into assets, vulnerabilities, and network behavior. Sees what is on the OT network.

+

DeRISK CRQ
Translates OT visibility into financial risk: Expected Loss, Value at Risk, 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 16 facilities across three regions (EU, Americas, Asia-Pacific), two business units, and three generation technologies — wind, solar, and combined-cycle gas.

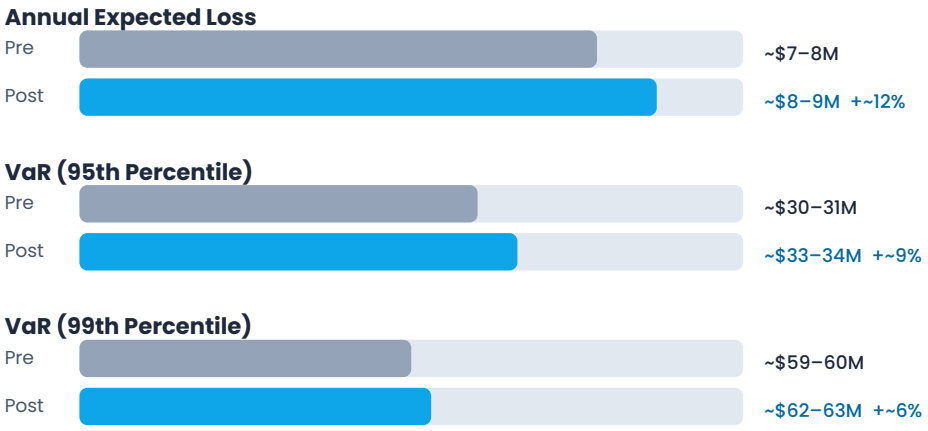
1. Quantify annual cyber risk for the full portfolio
2. Ingest OT IDS telemetry and measure its impact on risk quantification
3. Compare Pre- vs. Post-OT telemetry results
4. Compare risk across regions, sub-industries, and business entities
5. Simulate six risk mitigation projects and quantify their risk reduction
6. Deliver results in financial terms usable by the Risk Committee and Board

All six criteria achieved

RESULTS

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

After OT IDS 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.



Key Insight: More visibility > more discovered vulnerabilities > higher (more accurate) risk quantification. Without CRQ, the company would have seen more alerts but not known what they meant for the bottom line.

RESULTS

Telemetry Impact by Region

Americas

Full Telemetry

EL increased ~40%

VaR 99th increased ~70%

Most accurate risk picture — telemetry revealed previously hidden exposure.

EU

No Telemetry Yet

EL appeared to decrease

Model less granular

Without telemetry, regional calibration masks real risk. IDS deployment underway.

Asia-Pacific

Telemetry Active

EL decreased slightly

Lower attack exposure

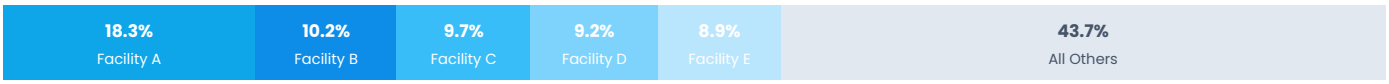
Regional threat context matters — telemetry + calibration drive accuracy.

Takeaway: Telemetry fundamentally changes the accuracy of risk quantification. Regions without it are flying partially blind.

RESULTS

Portfolio Risk Concentration

Portfolio-level CRQ reveals which assets deserve investment priority — not based on gut feel, but on quantified financial exposure.



5 facilities (31% of portfolio) = 56% of total Annual Expected Loss

Risk by Generation Technology

RESULTS

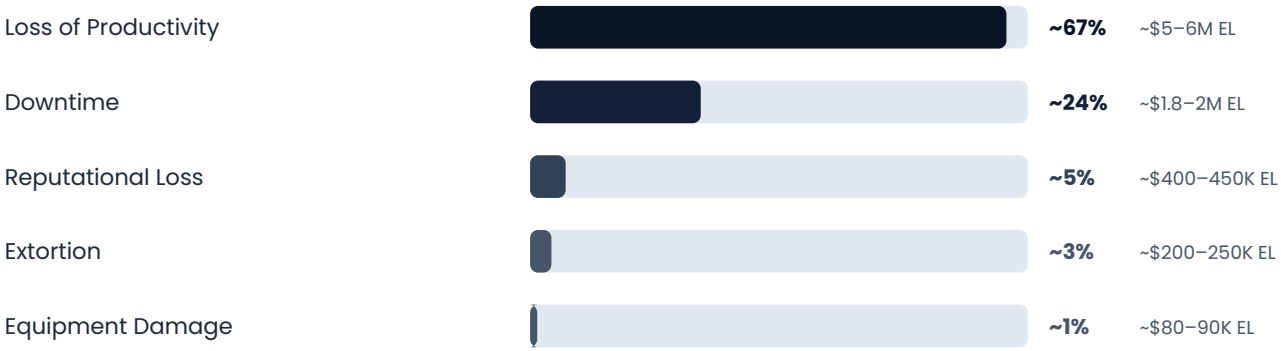
Drivers of Cyber Risk

DeRISK CRQ maps your OT platform's vulnerability data 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.

Top Initial Access Vectors (MITRE ATT&CK mapped)

Remote service exploitation accounts for over 60% of total expected loss. Spear phishing — often the focus of training budgets — ranks 5th at ~6%. DeRISK CRQ redirects investment to the vectors that actually drive loss.

Top Loss Events



Productivity loss + downtime = ~90% of expected annual loss. Equipment damage — often the assumed worst case — is ~1%.

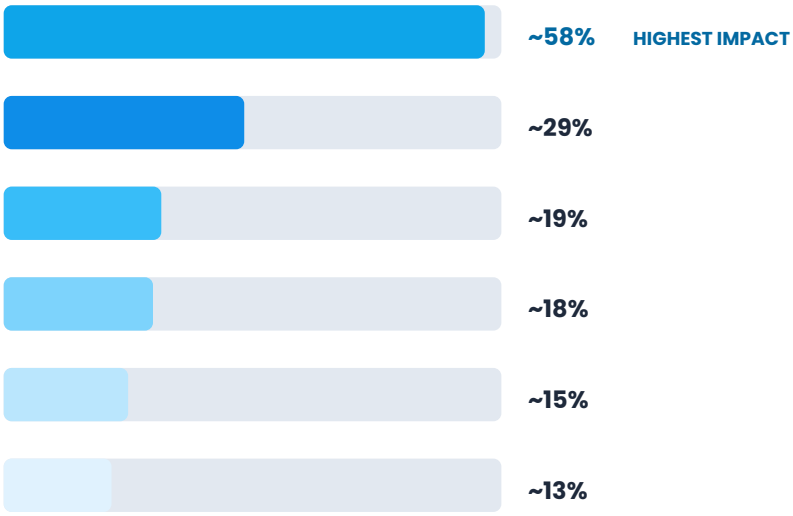
RESULTS

Mitigation ROI Simulation

Six security investment projects were defined and simulated against the highest-risk facility using DeRISK CRQ's Project Simulator. Each project's impact was quantified in dollars — enabling an apples-to-apples comparison that no qualitative framework can provide.

Risk Reduction by Project

(Expected Loss reduction, single facility)



Key Insight

The highest-impact project wasn't technical — it was operational. Business continuity and disaster recovery planning delivered nearly 2× the risk reduction of the next-best option.

Without DeRISK CRQ's financial quantification, this project would likely have been deprioritized in favor of more visible technical investments.

Detail: BCP, CMP & Disaster Recovery Project

~58% EL Reduction	**~53%** VaR 99th Reduction	**~68%** VaR 95th Reduction
12 Controls in Scope	**1 per control** Maturity Delta	**30 days** Timeline

THE BIGGER PICTURE

From a Dozen Facilities to 200+

~12
Facilities assessed
Engagement scope

200+
Facilities in portfolio
Full deployment potential

Extrapolation suggests enterprise-wide Value at Risk could be an order of magnitude higher than the engagement scope alone. This isn't a prediction — it's a reason to scale. The engagement proved the methodology; full deployment provides the enterprise number.

"If a dozen facilities carry this level of risk, what does the full portfolio look like?"

OUTCOME

Three-Pronged Risk Strategy

DeRISK CRQ enabled a comprehensive risk strategy that goes beyond mitigation alone:

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 defensible, 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 regions to close the telemetry gap
- Expand DeRISK CRQ from initial scope to full global portfolio
- Adopt periodic CRQ cycles for all business entities
- 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 (EL) 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 weeks, one engagement turned a dozen facilities' worth of OT data into a quantified risk picture that reached the boardroom —

and a prioritized investment roadmap that could cut the highest-risk facility's expected loss by more than half.

Ready to quantify your OT cyber risk?

denexus.io

DENEXUS™

DeRISK CRQ — Cyber Risk Quantification for Industrial Enterprises