CASE STUDY

Better Together:

Continuous Cyber Risk Quantification Meets OT Visibility

How a leading renewable energy company turned Your OT IDS + OT Firewall visibility into quantified financial risk across 64 industrial facilities — and proved which security investments actually reduce loss.

DENEXUS

DeRISK CRQ | DeRISK QVM

CUSTOMER PROFILE

A Leading Renewable Energy Company

Americas
Region of Operations

64
Facilities
31 Wind | 33 Solar

~7,600 MW
Total Generation Capacity

The company had deployed Your OT IDS + OT Firewall across 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 OT platforms tell you what's on your network. But who tells your board what it costs?

Vulnerability ≠ Financial Risk

10,576+ CVEs identified across 64 facilities — but security teams had no way to express that exposure in dollars.

No Portfolio-Wide Risk Metric

64 facilities across wind and solar sub-portfolios with no common financial benchmark for comparison.

Your OT IDS + OT Firewall Impact Unquantified

Your OT IDS + OT Firewall was deployed, but nobody could answer: did it change the financial risk picture? By how much?

No ROI for Mitigation Spend

Four security projects competed for budget with no way to rank them by risk reduction per dollar.

Board Communication Gap

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

NERC CIP compliance requirements added urgency — but proactive risk management, not compliance, was the primary driver.

THE SOLUTION

DeRISK CRQ + DeRISK QVM + Your OT IDS + OT Firewall + your OT firewall platform

Your OT IDS Provides	What It Captures	What DeRISK CRQ + QVM Does With It
Your OT IDS Asset Inventory	OT devices, protocols, CVEs — all 64 facilities	Builds facility-specific risk models; QVM ranks vulnerabilities by financial impact
Your OT IDS Network Behavior	Traffic patterns, connectivity, anomalies	Calibrates attack probability models with real network topology data
your OT firewall platform Firewall Rules	Inbound/outbound traffic, rule sets (11 of 64 facilities)	Refines attack path analysis with actual network segmentation data

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.

What DeRISK CRQ + QVM Delivers

- Portfolio risk aggregation across all 64 facilities
- Loss event financial breakdown by type
- QVM: CVE prioritization by financial exposure
- MITRE ATT&CK attack vector decomposition
- Mitigation ROI simulation (Project Simulator)
- Continuous quarterly risk monitoring cycles

The "Better Together" Thesis

Your OT IDS

OT IDS: asset inventory, CVE detection, and network behavior across 64 facilities. Firewall telemetry via your OT firewall platform for 11 sites. Sees what is on the network — assets, vulnerabilities, traffic patterns.

+

DeRISK CRQ + QVM

Translates OT visibility into quantified financial risk: Expected Loss, Value at Risk, and attack vector decomposition. DeRISK QVM ranks each CVE by its contribution to Expected Loss — not CVSS score — enabling financially-driven remediation prioritization.

=

Together

See the network. Quantify risk in dollars. Prioritize remediation by financial impact. Prove the ROI of every security investment. The full loop — visibility and quantification working as one.

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

ENGAGEMENT SCOPE

Scope & Success Criteria

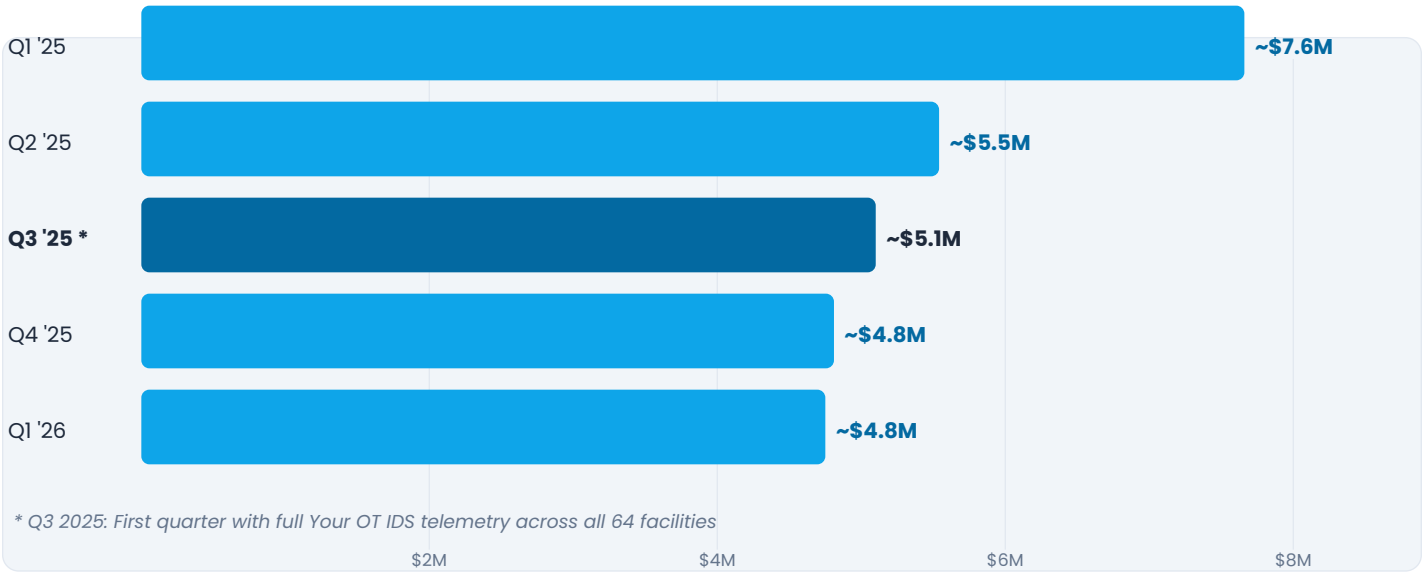
01 Quantify annual cyber risk for the full 64-facility portfolio using DeRISK CRQ
02 Ingest Your OT IDS asset and CVE telemetry; measure its impact on risk quantification
03 Expand DeRISK QVM to full portfolio — rank all 10,576+ CVEs by financial exposure
04 Segment risk across Wind vs. Solar sub-portfolios and OEM vs. non-OEM classifications
05 Simulate four risk mitigation projects and quantify their AEL and VaR reduction
06 Deliver results in financial terms for quarterly Risk Committee reporting

All six criteria achieved

KEY RESULTS

Five-Quarter AEL Trend — Continuous Monitoring in Action

~$7–8M	~$27M	~$59M
Baseline AEL (Q1 2025)	VaR 95th (1-in-20 year)	VaR 99th (1-in-100 year)



-38% reduction in Annual Expected Loss from Q1 2025 to Q1 2026

RESULTS

The Your OT IDS Effect: From Partial to Full OT Visibility

Before — Q2 2025 (Partial Telemetry)

- 15 of 64 facilities with CVE data
- 242 distinct CVEs in scope
- 4 CVEs driving most financial risk
- 413 devices impacted by top CVEs
- Portfolio risk: ~$5.5M AEL

After — Q3 2025 (Full Your OT IDS Telemetry)

- All 64 facilities with CVE data
- 10,576 total CVEs detected
- 389 distinct CVEs identified
- 83 risky CVEs (21.3% risky/distinct ratio)
- 18 CVEs in CISA KEV catalog

Key Insight

Full OT telemetry doesn't just improve the model — it changes the financial picture. Risks that were invisible become quantified. DeRISK QVM then ranks each of the 83 risky CVEs by their contribution to Expected Loss, not by CVSS score, enabling the security team to prioritize remediation by dollar impact — not by technical severity alone.

10,576	389	83	20	79%
Total CVEs across 64 facilities	Distinct CVEs identified	Risky CVEs (21.3% of distinct)	CVEs in CISA KEV catalog	Risk driven by top 5 CVEs

DERISK QVM INSIGHT

Financial Prioritization — Which CVEs Matter Most

Top 5 CVEs drive 72–79% of total financial risk
Just 5 of 389 distinct CVEs account for the vast majority of portfolio Expected Loss.

2 CVEs match industry top-10 peer benchmarks
CVE-2017-9765 and CVE-2013-0006 appear in DeNexus peer database top 10 for Power Generation.

4 CVEs in 413 devices = majority of addressable risk
QVM concentrates remediation effort on the highest-leverage targets across wind and solar fleets.

RESULTS

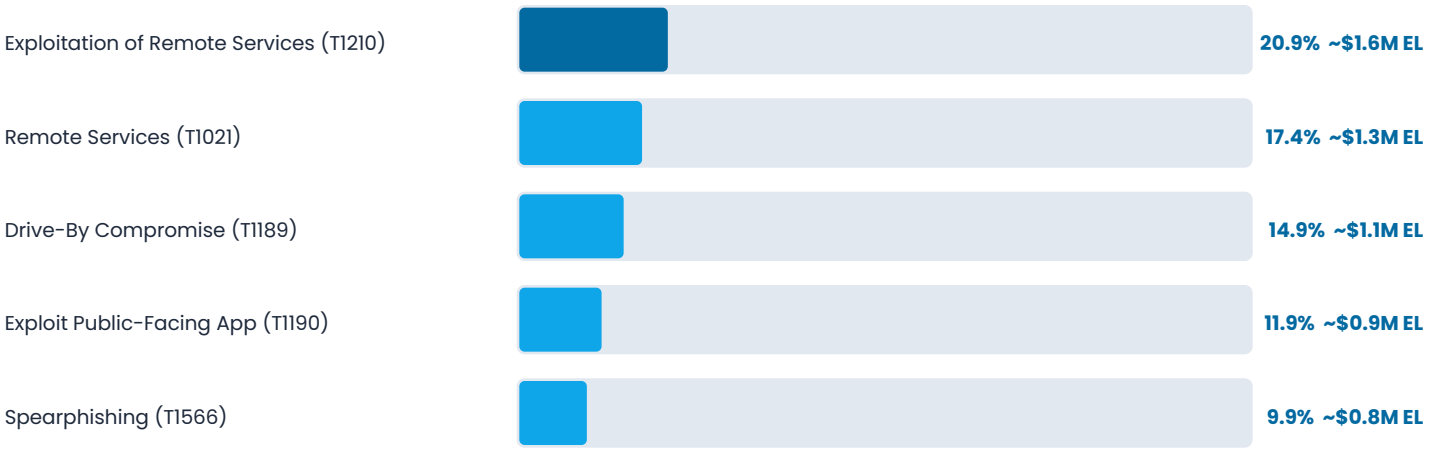
Portfolio Risk Concentration & Drivers of Loss

~80%	~21%	~78%	~22%
Solar Portfolio	Wind Portfolio	Non-OEM Managed	OEM-Managed
33 plants, ~3,500 MW	31 plants, ~4,100 MW	35 plants, higher exposure	29 plants, lower exposure

Solar Large 200-399 MW (5 facilities) accounts for 56.7% of total portfolio AEL — the highest-concentration sub-portfolio.

RISK DRIVERS

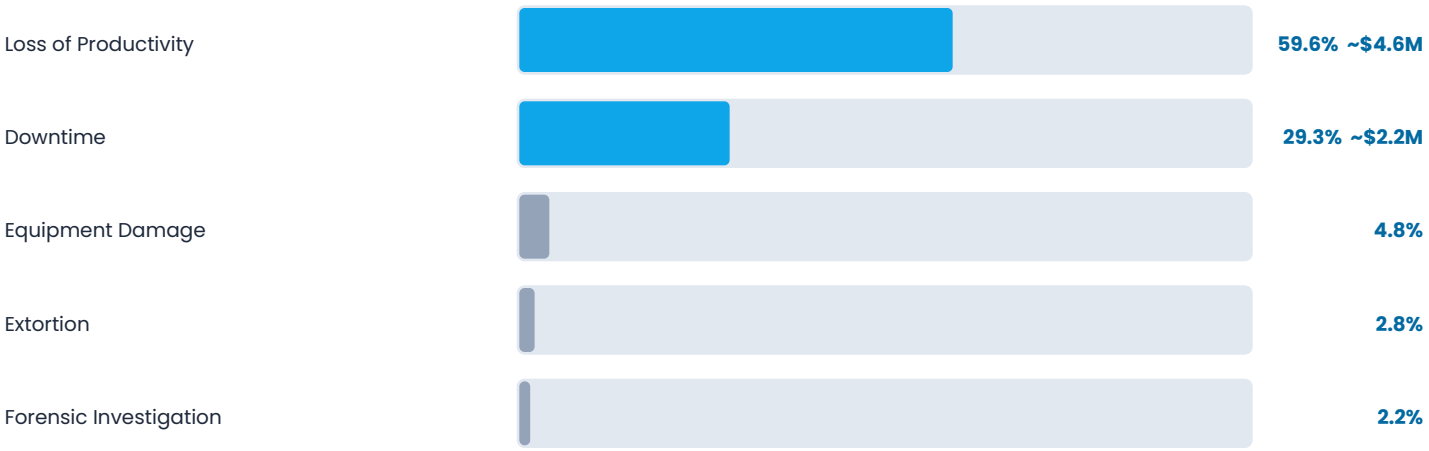
Top Initial Access Vectors (MITRE ATT&CK Mapped)



Remote service exploitation drove >60% of EL at baseline. By Q3 2025, Spearphishing rose to #1 as full CVE telemetry revealed additional exposure.

LOSS EVENTS

Top Loss Categories by Expected Annual Loss



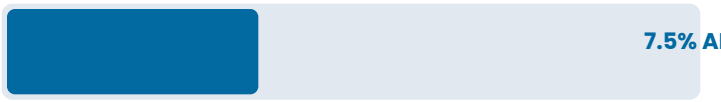
Productivity loss + downtime = ~89% of expected annual loss. Equipment damage — often assumed worst case — represents less than 5%.

RESULTS

Risk Mitigation Roadmap — ROI Simulation

Four security investment projects were defined across a two-year roadmap and simulated 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.

2025 Security Program



7.5% AEL reduction

- Plant Active Directory — Centralized auth, LDAP, RODCs, DNS, NTP
- Privileged Access Management — Intermediary for OT remote access

2026 Security Program

+10.7% additional reduction

- Disaster Recovery & Backups — Ransomware recovery, config management, BIA
- Endpoint Hardening — Least privilege, change control, secure deployment

Combined 2025 + 2026 Programs — **18.2% Total AEL Reduction**

Key Insight

The 2026 Disaster Recovery & Backups program delivers the highest single-year risk reduction of the four projects — because ransomware recovery capability cuts the tail-risk loss events that drive VaR 99th. Without DeRISK CRQ's financial quantification, this project would likely have been deprioritized in favor of more visible technical controls.

18.2%	~$1.4M	~$6.4M
Total AEL Reduction	Annual Savings (AEL Delta)	Reduction in Insured Limit Post-mitigation: ~$20M insured

THE BIGGER PICTURE

From 64 Facilities to a 300+ Implementation Benchmark

64
Facilities Assessed
~7,600 MW

›

300+
DeRISK CRQ Implementations
Industry benchmark for comparison

With 300+ CRQ implementations across the industrial sector, DeNexus benchmarks each facility against peers by sector and technology. Every quarterly cycle adds to that benchmark.

"Five quarters of continuous monitoring turned a 64-facility OT estate into a quantified, board-ready risk picture — with a clear roadmap to reduce it."

Mitigate

Use CRQ to continuously evaluate risk exposure and simulate mitigation strategies with quantified ROI. QVM prioritizes which CVEs to remediate first.

Transfer

Use CRQ outputs to optimize cyber insurance coverage and negotiate with brokers using defensible, data-backed risk figures. $6.4M reduction in insured limit achieved.

Accept

For risks below threshold, quantify the acceptance level in dollar terms. DeRISK CRQ replaces qualitative judgment with defensible financial thresholds.

OPERATIONAL NEXT STEPS

Continuing the Journey

- Complete Your OT IDS telemetry ingestion for all remaining facilities in portfolio
- Expand your OT firewall platform firewall data integration from 11 to all 64 facilities
- Continue quarterly CRQ + QVM cycles for all sub-portfolios and business units
- Use DeRISK QVM to track CVE remediation velocity and financial risk impact over time

REFERENCE

Glossary of Terms & Acronyms

Acronym	Full Term	Definition
AEL	Annual Expected Loss	See EL. Used interchangeably with Expected Loss (EL) in most contexts.
BCP	Business Continuity Plan	A documented strategy ensuring critical business functions continue during and after a disruption.
CISA KEV	CISA Known Exploited Vulnerabilities	CISA's catalog of CVEs with confirmed real-world exploitation. Presence = highest remediation priority.
CMP	Crisis Management Plan	Framework for organizational response to a significant incident: communication, escalation, decision authority.
CRQ	Cyber Risk Quantification	The process of expressing cyber risk in financial terms (dollars), enabling comparison with other business risks.
CVE	Common Vulnerability & Exposure	A standardized identifier for a known cybersecurity vulnerability in hardware or software.
CVSS	Common Vulnerability Scoring System	A technical severity score (0-10) for CVEs. Does not reflect financial impact or exploit probability.
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. Used for budgeting, insurance sizing, and baseline risk communication.
IDS	Intrusion Detection System	A network security tool that monitors traffic for suspicious activity. In OT contexts, provides asset inventory and CVE detection.
MITRE ATT&CK	Adversarial Tactics, Techniques & Common Knowledge	A globally recognized knowledge base of adversary behaviors, used to classify attack vectors by real-world prevalence and financial impact.
NERC CIP	NERC Critical Infrastructure Protection	Mandatory reliability standards for bulk electric system cybersecurity in North America.
OT	Operational Technology	Hardware and software that monitors and controls physical processes (SCADA, PLCs, DCS).
QVM	Quantified Vulnerability Management	DeNexus product that ranks CVEs by their contribution to Expected Loss — not CVSS score — enabling financially-driven remediation prioritization.
VaR	Value at Risk	Maximum annual loss expected at a given confidence level. VaR 95th = 1-in-20 year event. VaR 99th = 1-in-100 year event.
VaR 95th	Value at Risk, 95th Percentile	Maximum loss expected with 95% confidence. Informs insurance coverage and risk transfer decisions.
VaR 99th	Value at Risk, 99th Percentile	Maximum loss expected with 99% confidence. Drives board-level capital allocation and catastrophic scenario planning.

In five quarters, one continuous deployment turned 64 facilities' worth of OT data into a quantified risk picture that reached the Risk Committee —

and a data-driven roadmap that is reducing the portfolio's expected annual cyber loss by more than 18%.

Ready to quantify your OT cyber risk?
denexus.io

DENEXUS™

DeRISK CRQ | DeRISK QVM — Cyber Risk Quantification for Industrial Enterprises