CASE STUDY

Better Together:

Continuous Cyber Risk Quantification Meets OT Visibility in T&D

How a leading European transmission system operator turned Nozomi Networks OT visibility into quantified financial risk across 3 industrial substations — and proved which security investments actually reduce loss.

DeNexus
DeRISK CRQ

CUSTOMER PROFILE

A Leading European Transmission System Operator

1 Region	3 Substations	9 Weeks	NIST CSF 2.0
EU	Transmission Grid Assets	Engagement Duration	Early Adopter

The company had deployed Nozomi Networks IDS across its OT environment to gain visibility into assets and vulnerabilities. The next step: translating that technical visibility into financial risk 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-Asset Comparison

Individual substations operated without a common risk metric, making portfolio-level decisions impossible.

IDS Impact Unquantified

Nozomi was deployed, but nobody could answer: did it change the risk picture? By how much?

No ROI for Mitigation Spend

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

Communication Gap

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

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

THE SOLUTION

DeRISK CRQ + Nozomi Networks

Nozomi Networks 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.

Nozomi 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 substation risk to network or enterprise level

Attack Vector Decomposition
MITRE ATT&CK techniques driving financial risk

Loss Event Breakdown
Productivity loss, downtime, reputational damage, extortion

Mitigation Simulation
Forecast risk reduction and ROI of proposed security investments

The "Better Together" Thesis

Your OT Platform
Asset inventory
Vulnerability detection
Network behavior
Traffic anomalies

+

DeRISK CRQ
Annual Expected Loss
Value at Risk (VaR)
MITRE ATT&CK mapping
Mitigation ROI

=

Together
See the environment
Quantify risk 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

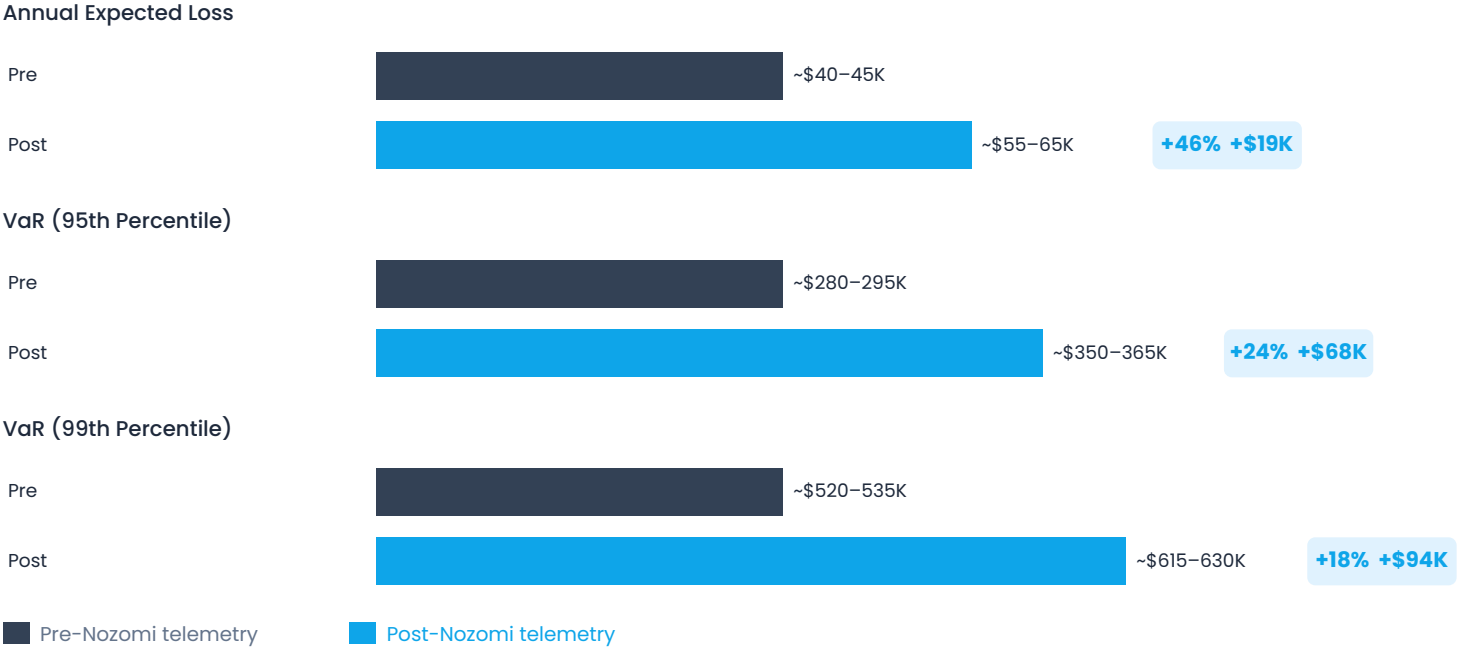
1. Quantify annual cyber risk (EL and VaR) for all 3 substations
2. Ingest Nozomi telemetry and measure its impact on risk quantification accuracy
3. Compare Pre- vs. Post-Nozomi results across all risk metrics
4. Analyze interdependencies between substations within the transmission mesh
5. Simulate 3 risk mitigation projects and quantify their dollar-denominated risk reduction
6. Deliver results in financial terms usable by the Risk Committee and board

All 6 criteria achieved

RESULTS

The Nozomi Effect: Pre- vs. Post-Telemetry

After Nozomi telemetry was ingested, portfolio risk increased — and that's the point. Previously invisible vulnerabilities surfaced, and DeRISK CRQ translated them into precise financial deltas across every risk metric.



Key Insight
More visibility reveals more vulnerabilities — producing a higher, more accurate risk figure. Without CRQ, the company would have seen more alerts but not known what they meant for the balance sheet.

RESULTS

Portfolio Risk Concentration by Substation

Portfolio-level CRQ reveals which assets deserve investment priority — not based on gut feel, but on quantified financial exposure. Substation A drives 36% of total EL despite representing one of only three assets in scope.

Substation A

36.29%

of total Annual Expected Loss

~$21–23K EL

Top risk contributor

Remote service exploitation and reputational exposure are the dominant drivers.

Substation B

1.83%

of total Annual Expected Loss

~$1.0–1.2K EL

Moderate exposure

Lower asset count and reduced connectivity limit attack surface relative to Substation A.

Substation C

0.22%

of total Annual Expected Loss

~$125–145 EL

Minimal exposure

Smallest substation in scope. Very low individual asset risk; impact felt at portfolio level.

RISK ALLOCATION (ANNUAL EXPECTED LOSS)

Substation A drives the majority of the addressable substation-level risk

Note on loss attribution: Company-level events (reputational loss, forensic) account for ~62% of total EL — recorded above substation level, reflecting the systemic nature of grid outages.

NOTE ON LOSS ATTRIBUTION

In DeRISK CRQ's T&D model, reputational loss and forensic investigation costs are attributed at the enterprise level rather than to individual substations — reflecting the systemic nature of grid outages. These company-level events account for approximately 62% of total Annual Expected Loss, with the remaining 38% distributed across individual substations.

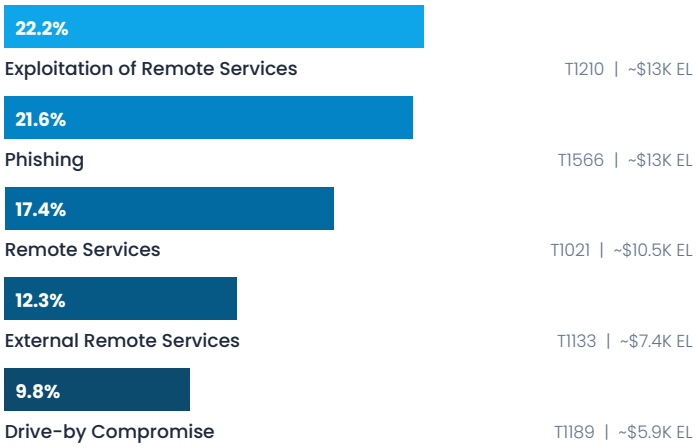
RESULTS

Drivers of Cyber Risk

DeRISK CRQ maps Nozomi'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)

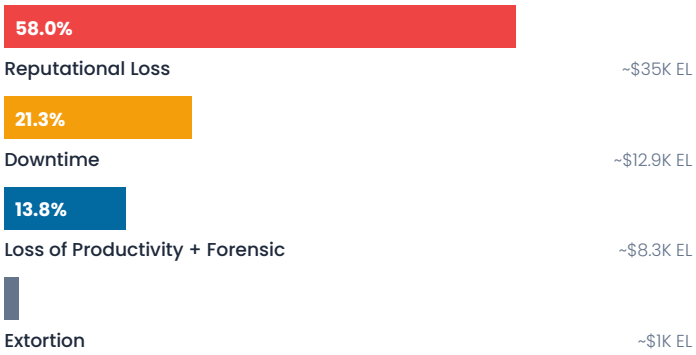
Contribution to Annual Expected Loss



T&D Insight:
Phishing ranks #2 (22%) in T&D — far higher than in generation environments. Remote service exploitation + phishing together account for ~44% of total EL.

Top Loss Events

Contribution to Annual Expected Loss



T&D vs. Generation:
Reputational loss dominates at 58% in T&D — the reverse of generation environments (where productivity loss leads at 67%). Grid outages carry disproportionate regulatory and public consequences.

RESULTS

Mitigation ROI Simulation

Three security investment projects were defined and simulated against the highest-risk substation 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 (VAR 95TH PERCENTILE)

~7.5%
~$26–27K VaR reduction

HIGHEST IMPACT

Backup & Recovery

~1.1%
~$3.5–4.5K VaR reduction
Remote System (Secure Access)

~0.8%
~$2.5–3.5K VaR reduction
Awareness & Training

Key Insight — Why Backup & Recovery Outperforms

Backup & Recovery directly reduces the severity of impact — specifically, the duration and cost of downtime while systems are restored. This has immediate, dollar-denominated effect on VaR.

Remote access controls, by contrast, reduce the probability of exploit — a different risk mechanism. Probability reduction has a less direct financial effect than severity reduction, which is why the $60K Backup & Recovery outperforms the $150K Remote System on VaR.

Without DeRISK CRQ's financial quantification, the more visible technical investment would likely have won the budget — leaving the highest-ROI project unfunded.

DETAIL: BACKUP & RECOVERY PROJECT

~7.5% VaR 95th Reduction	**~7.4%** VaR 99th Reduction	**~8.2%** EL Reduction
~$26–27K VaR 95th Delta	**$60K** CAPEX	**2 months** Implementation

THE BIGGER PICTURE

From 3 Substations to an Enterprise-Wide View

3 Assessed — **Full Portfolio**

The assessment proved the methodology across 3 substations. Full enterprise-wide deployment provides the complete risk picture — and the defensible numbers that boards, risk committees, and insurers require.

"If 3 substations carry this level of risk, what does the full enterprise look like?"

OUTCOME

Three-Pronged Risk Strategy

Mitigate

Use CRQ to continuously evaluate risk exposure and simulate mitigation strategies with quantified ROI — so every security investment is defensible.

Transfer

Use CRQ outputs to optimize cyber insurance coverage and negotiate with brokers using data-backed, quantified risk figures rather than qualitative assessments.

Accept

For risks below threshold, quantify the acceptance level in dollar terms rather than relying on qualitative judgment — and document it for governance purposes.

OPERATIONAL NEXT STEPS

- Complete Nozomi IDS deployment across all remaining network segments to close the telemetry gap
- Expand DeRISK CRQ from the initial 3-substation scope to full enterprise deployment
- Adopt periodic CRQ cycles for all business units and regulatory reporting cycles
- Use Project Simulator for ongoing mitigation planning and budget justification with the board

REFERENCE

Glossary of Terms & Acronyms

Key terms and acronyms used throughout this case study and in DeRISK CRQ reporting.

Acronym	Full Term	Definition
AEL	Annual Expected Loss	The average annual cyber loss across thousands of simulated scenarios. Synonymous with EL.
BCP	Business Continuity Plan	Policies and procedures ensuring critical operations continue during and after a disruptive event.
CMP	Crisis Management Plan	A structured response framework for managing the communication and decision-making during a crisis.
CRQ	Cyber Risk Quantification	The process of expressing cyber risk in financial terms — dollars, confidence intervals, and probabilities.
DRP	Disaster Recovery Plan	Technical procedures for restoring IT/OT systems and data after an incident or failure.
EL	Expected Loss	The most probable annual cyber loss in dollars. The baseline metric for budgeting and insurance sizing.
IDS	Intrusion Detection System	A tool that monitors OT/IT networks for malicious activity, policy violations, and anomalous behavior.
MITRE ATT&CK	MITRE Adversarial Tactics, Techniques & Common Knowledge	A globally recognised framework cataloguing adversary tactics and techniques observed in real-world attacks.
OT	Operational Technology	Hardware and software that monitors and controls physical devices, processes, and infrastructure.
VaR	Value at Risk	The maximum expected loss at a given confidence level over a defined time period (typically one year).
VaR 95th	Value at Risk — 95th Percentile	The maximum annual loss expected to be exceeded only once every 20 years (1-in-20 year event).
VaR 99th	Value at Risk — 99th Percentile	The maximum annual loss expected to be exceeded only once every 100 years (1-in-100 year event).

Source: DeRISK CRQ platform documentation and MITRE ATT&CK framework (mitre.org/attack).

In 9 weeks, one assessment turned 3 substations' worth of OT data into a quantified risk picture that reached the boardroom —

and a prioritized investment roadmap that proved the highest-impact project wasn't the most expensive.

Ready to quantify your OT cyber risk?

denexus.io

DeNexus

DeRISK CRQ | Cyber Risk Quantification for Industrial Enterprises