DENEXUS | NOZOMI NETWORKS

3 substations | EU | 9-week assessment | NIST CSF 2.0

CASE STUDY

Better Together: Continuous Cyber Risk Quantification Meets OT Visibility in T&D

DeNexus™ | DeRISK CRQ v5 | With Nozomi Networks

THE CUSTOMER

A leading European transmission system operator with 3 industrial substations (EU) serving a high-voltage transmission grid. It had deployed the Nozomi Networks Platform across its OT environment to see assets, vulnerabilities and network behavior.

THE CHALLENGE

The Nozomi Networks Platform gave OT visibility but could not turn vulnerability data into financial risk. There was no common metric across substations and no way to rank 3 competing security projects by ROI. NIS 2 added urgency, but proactive risk management was the main driver.

THE SOLUTION

DeRISK™ CRQ v5 ingested Nozomi Networks' asset, vulnerability and network data. It turned them into quantified financial risk: Annual Expected Loss, Value at Risk, MITRE ATT&CK-mapped attack vectors and mitigation ROI simulation across all 3 substations.

BETTER TOGETHER

Nozomi Networks: assets, vulnerabilities, network behavior.

DeRISK CRQ v5: Expected Loss, Value at Risk, mitigation ROI.

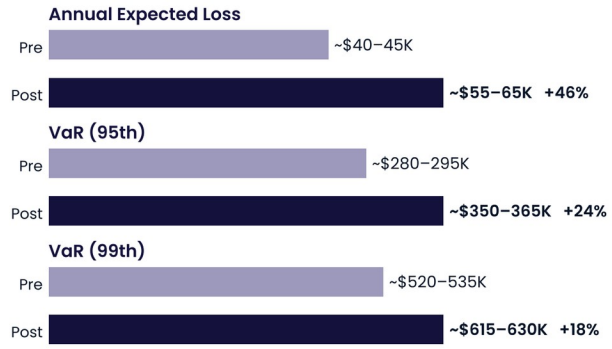
Together: see, quantify, prioritize, prove. Visibility alone does not reduce risk.

MITIGATION ROI SIMULATION (VAR 95TH REDUCTION)



Backup & Recovery reduces how severe an incident is (magnitude). Remote access controls reduce how likely an exploit is (frequency), a less direct financial effect. The $60K Backup & Recovery project beats the $150K Remote System project on VaR.

KEY RESULTS



Pre- vs. post-telemetry | 3 substations | EU

36.29%
Risk concentration
of total EL from Substation A alone

>60%
Top attack vectors
of EL from remote service exploitation + phishing

~58%
Top loss event
of expected loss from reputational damage

RISK DRIVERS (SHARE OF EL)



THE BIGGER PICTURE

3 substations assessed. Full enterprise deployment gives the board-ready risk picture and the defensible numbers risk committees and insurers need.

NEXT STEPS

- Complete deployment of the Nozomi Networks Platform across remaining network segments
- Expand cyber risk quantification to the full enterprise
- Use the DeRISK Scenario Simulator for ongoing board budget planning

STRATEGY

Mitigate, **transfer** or **accept** each risk with dollar-based evidence.

Glossary **EL / AEL** Annual Expected Loss: the most probable annual cyber loss in dollars. **VaR** Value at Risk: loss expected once per 20 years (95th) or 100 years (99th). **BCP** Business Continuity Plan. **CMP** Crisis Management Plan. **CRQ** Cyber Risk Quantification. **OT** Operational Technology.

About Nozomi Networks Nozomi Networks protects the world's critical infrastructure from cyber threats. Our platform uniquely combines network and endpoint visibility, threat detection, and AI-powered analysis for faster, more effective incident response. Customers rely on us to minimize risk and complexity while maximizing operational resilience. www.nozominetworks.com

Nozomi Networks sees the network. DeRISK CRQ v5 counts the cost. Together, the full picture. **denexus.ai**

© 2026 DeNexus, Inc. DeNexus and DeRISK are trademarks of DeNexus, Inc.