Northwind Manufacturing Co.

Manufacturing · Executive Risk Assessment · Ransomware on air-gapped OT — sample analysis · 2026-05-07

Control Value: $400k

50% reduction in annualized loss expectancy

For Ransomware via removable media (air-gapped OT), the current control posture reduces annualized loss expectancy by $400,000, bringing residual ALE to $400,000. This estimate reflects 10,000 Monte Carlo iterations. These are modeled estimates shown as ranges, not measured or guaranteed loss reductions.

Run UUID: edb51d38-8a34-41ad-9495-77bd5a0d39b0 · Generated by Idraa

Contents

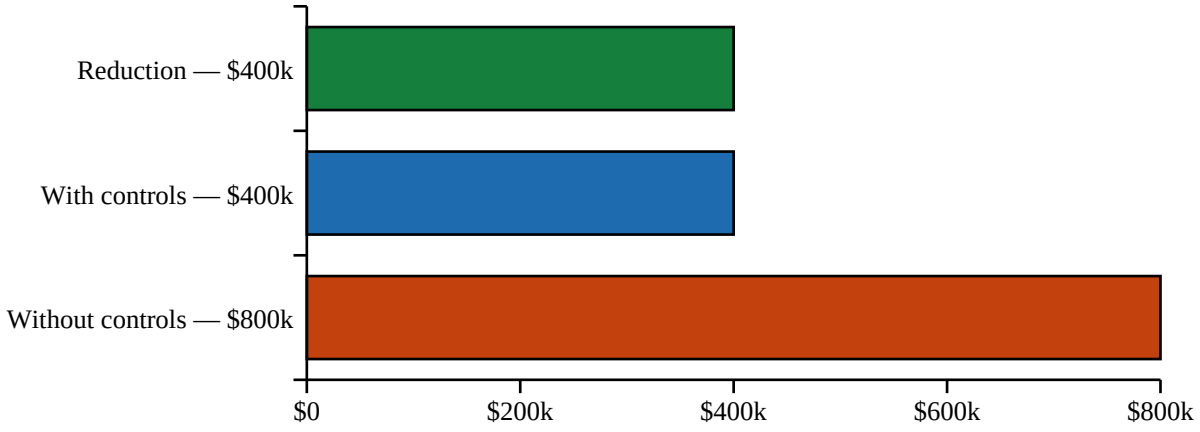
Risk picture

$400k

Central 95% of modeled annualized losses: $300k – $520k

Annualized loss expectancy with current control posture.

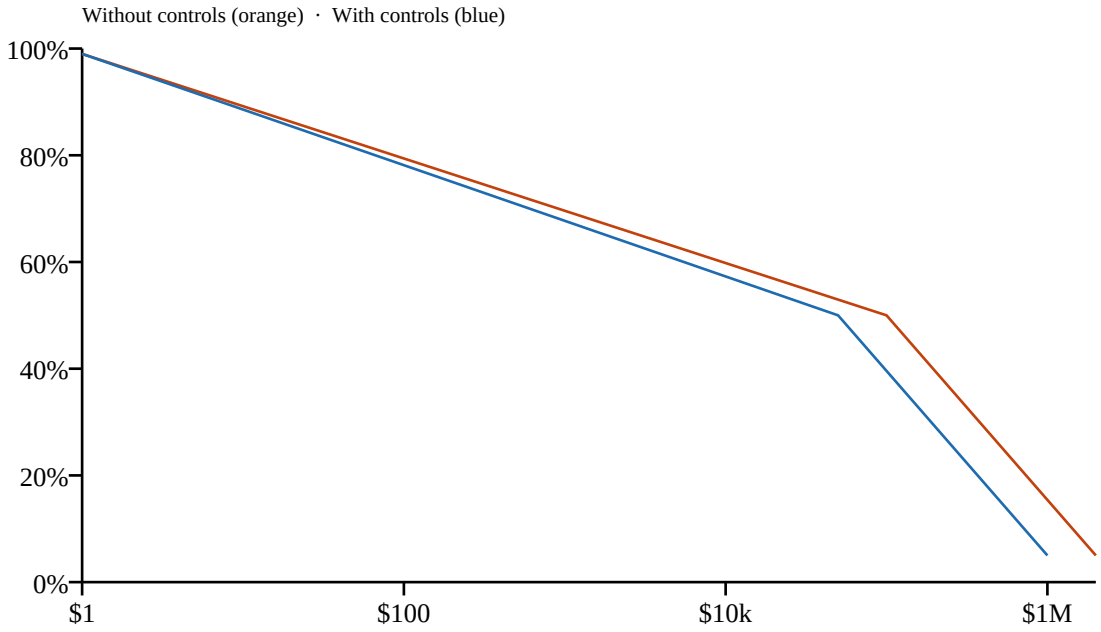
Risk comparison



Estimates are derived from 10,000 Monte Carlo iterations (single scenario).

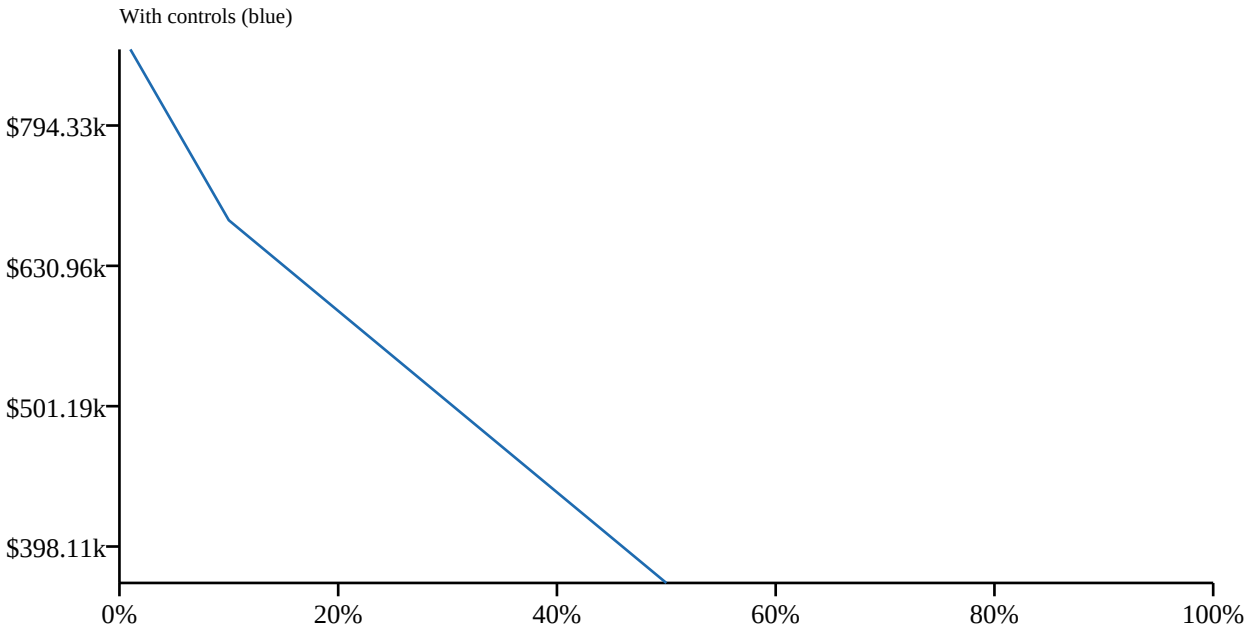
Loss distributions — Ransomware on air-gapped OT — sample analysis

Loss Exceedance Curve (LEC)



P(annual loss ≥ X) at each loss level.

Exceedance Probability Curve (EPC)



At each percentile X, simulated loss is $Y.

Distribution statistics & tail risk

Metric	Without controls *(base)*	With controls *(residual)*	Δ (base - residual)
Mean (average)	$820k	$410k	+$410k
Typical case (median)	$750k	$375k	+$375k
Std deviation	$200k	$100k	+$100k
1-in-10 year (VaR 90%)	$1.10M	$580k	+$520k
1-in-20 year (VaR 95%)	$1.30M	$680k	+$620k
1-in-100 year (VaR 99%)	$1.80M	$900k	+$900k
1-in-1000 year (VaR 99.9%)	$2.50M	$1.20M	+$1.30M
Expected shortfall (95%)	$1.45M	$750k	+$700k
Expected shortfall (99%)	$1.95M	$1M	+$950k
Expected shortfall (99.9%)	$2.70M	$1.30M	+$1.40M

VaR_q: q-th percentile of simulated annual loss (empirical). ES_q: mean simulated annual loss at or above the q-th percentile (empirical).

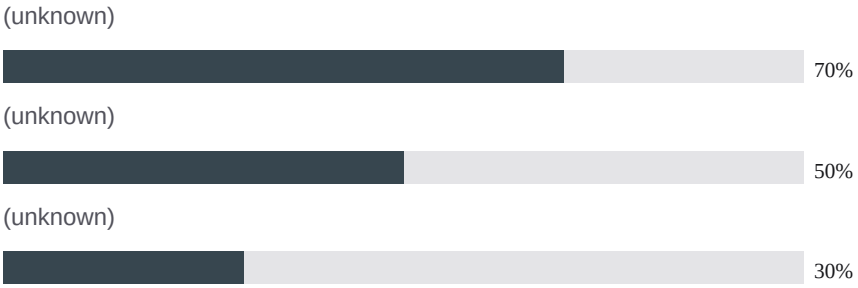
"1-in-T year" denotes an annual loss with a 1/T probability of being exceeded (VaR at the (1-1/T) percentile) - an expected recurrence interval, not a fixed cycle or a cap.

Control economics

KPI	Value
Total annual cost	$100k
Risk reduction	$400k
Net benefit	$300k
ROI	4.00x

These are modeled estimates shown as ranges, not measured or guaranteed loss reductions.

Control effectiveness



Effectiveness: composite score (0-1) from the FAIR-CAM control model.

Assumptions & inputs

Organisation & run context

Organisation: Northwind Manufacturing Co.

Industry: Manufacturing

Annual revenue: not set

Loss tolerance: not set

Run type: Single scenario

Completed at: 2026-05-07 15:00 UTC

Simulations (n): 10,000

Random seed: not recorded

Engine: fair-cam 0.1.0

Input distributions (per scenario)

Ransomware via removable media (air-gapped OT)

Threat Event Frequency (TEF)

Distribution type: PERT (elicited values: low / most-likely / high)

Parameter	Value
Low	0.10 /yr
Most-likely (mode)	0.50 /yr
High	1.00 /yr

Vulnerability

Distribution type: PERT (elicited values: low / most-likely / high)

Parameter	Value
Low	20.0%
Most-likely (mode)	40.0%
High	60.0%

Primary Loss

Distribution type: PERT (elicited values: low / most-likely / high)

Parameter	Value
Low	$10k
Most-likely (mode)	$100k
High	$1M

Control-assignment snapshot

Values as captured at execution time (snapshot, not live controls). Unit type preserved to make capability values interpretable.

Control	Sub-function	Capability	Unit type	Coverage	Reliability	Confirmed
Firewall	—	—	—	—	—	—
EDR	—	—	—	—	—	—
SIEM	—	—	—	—	—	—

Methodology & provenance appendix

Scenario provenance

Ransomware via removable media (air-gapped OT)

analyst-authored — no library provenance

Vulnerability (inherent, pre-control baseline): analyst-authored — no library provenance

FAIR node glossary

TEF: Threat Event Frequency (TEF): the rate at which a threat agent is expected to act against an asset, expressed in events per year. TEF is an Open FAIR node in the Loss Event Frequency (LEF) component. It captures only the frequency of threat contact — not whether each contact results in a loss event.

Vulnerability: Vulnerability: the probability that a threat event results in a loss event, assessed BEFORE modeled controls are applied (inherent, control-naive baseline). Controls are applied on top of this baseline to derive the residual loss-event probability. The inherent baseline reflects the pre-control environment; reporting it as a post-control value would overstate the control benefit. Vulnerability is an Open FAIR node.

Loss Magnitude: Loss Magnitude (LM): the amount of loss resulting from a single loss event, combining Primary Loss (direct financial impact) and Secondary Loss (indirect and reputational costs such as regulatory fines, notification costs, and brand damage). Loss Magnitude is an Open FAIR node.

ALE: Annualized Loss Expectancy (ALE): E[LEF x LM] — the expected annual loss, computed as the expected product of loss-event frequency and loss magnitude across simulated outcomes. ALE is the primary risk metric reported by Idraa.

VaR: Value at Risk (VaR_q): the q-th percentile of simulated annual loss — the loss level that is not exceeded in q% of simulated years. VaR is not a FAIR Standard node — v3 view-model descriptive statistic, computed empirically from simulated outcomes. Common thresholds reported: VaR 90, VaR 95, VaR 99, VaR 99.9.

ES: Expected Shortfall (ES_q): the mean simulated annual loss at or above the q-th percentile — the average loss in the worst (100-q)% of simulated years (e.g. the worst 5% for q=95). ES is not a FAIR Standard node — v3 view-model descriptive statistic, computed empirically from simulated outcomes. Common thresholds reported: ES 95, ES 99, ES 99.9.

Simulation method

This report is based on Monte Carlo simulation with 10,000 iterations per run. All output (risk-result) percentile statistics — VaR, ES, loss exceedance percentiles — are empirical (computed from simulated outcomes), not parametric fits. Input distribution percentiles shown in the assumptions section are parametric, derived analytically from the specified lognormal parameters.

Control inventory

Loss Event Controls (LEC) (2)

Controls that act on loss events directly — prevention, detection, and response/recovery.

- Firewall *(preventive)*
- EDR *(preventive)*

Variance Management Controls (VMC) (1)

Controls that keep other controls reliable — monitoring, drift detection, and correction of control degradation.

- SIEM *(detective)*

Scenarios in this run

- Ransomware via removable media (air-gapped OT) — Ransomware via removable media (air-gapped OT) description for testing.

Run UUID: edb51d38-8a34-41ad-9495-77bd5a0d39b0 · Generated: 2026-05-07 15:00 UTC · 10,000 Monte Carlo iterations · Central 95% loss interval (p2.5–p97.5)
FAIR (Factor Analysis of Information Risk) — see Idraa run detail for full simulation output.

Generated by Idraa