CASE STUDY · HYPERSCALE DATA CENTERS · DeRISK CRQ

Quantifying the Full Risk Picture: Cyber and Physical Threats, One Financial Model.

How a leading hyperscale data center operator used DeRISK CRQ to quantify financial exposure from both network-based cyber attacks and physical security bypass — in a single model, expressed in dollars and MW/MWh.

MEAN ANNUAL EXPECTED LOSS

$4.77MM

1 hyperscale facility · 150MW

35% from physical attack paths

Full = 150MW at risk

DeRISK CRQ | Physical Security Model | OT Cyber Risk

The Challenge: Seeing the Full Risk Picture

CUSTOMER PROFILE

Industry:	Hyperscale Data Centers
Geography:	North America
Portfolio:	Multiple hyperscale facilities
Facility:	1 facility in scope · 150MW
OT Systems:	BMS · EPMS · PACS · DCIM
	Air & Water Handling
	Battery & Generator Backup
Framework:	NIST CSF — OT security posture
Engagement:	Ongoing DeRISK CRQ cadence

300+	10+	3
CRQ Deployments	Years OT Data	Continents

THE CHALLENGE

Siloed risk — no unified financial view

Data center operators face a growing and complex threat landscape. Cyber attacks targeting OT systems — building management, power, cooling, physical access — can trigger cascading failures. Physical security breaches compound the risk. Yet most manage these threats separately, with no common financial metric.

- **No unified financial model**
  Cyber and physical security assessments ran independently — findings could not be translated into a single, comparable risk number.
- **Unsustainable assessment cadence**
  Annual OT cyber assessments per facility were resource-intensive. Deep technical findings stayed in technical reports, never reaching board level.
- **Physical investment without ROI**
  Significant investment in perimeter security, access controls, and CCTV — but no methodology to quantify how much expected loss those controls were preventing.
- **Portfolio blind spot**
  With dozens of facilities across multiple regions, the operator lacked a portfolio-level risk view — no way to compare exposure across sites.

DeRISK CRQ with Physical Security Model

A single platform. Two attack surfaces. One financial model.

DeRISK CRQ quantifies financial exposure from OT cyber threats using the URMS (Unit Risk Modeling System) — a probabilistic engine combining attack frequency, attack path probability, and loss event impact. The Physical Security module was deployed alongside the standard cyber model, enabling financial quantification of physical attack paths for the first time.

LOSS ($) = NoA × APA × LEI | Frequency × Probability of Success × Financial Impact

NoA

Number of Attack Attempts

Estimates annual attack attempts per IAV using firmographics, threat intelligence, leaked credentials, and open ports.

Calibrated for high-revenue, high-attractiveness hyperscalers.

APA

Attack Path Algorithm

Simulates attack propagation through OT network zones to reach BMS, EPMS, PACS, DCIM.

Physical Security Phase 1 & 2 integrated — models physical bypass alongside network paths.

LEI

Loss Event Impact

Translates attacks into $:

- Equipment Damage
- Extortion
- Loss of Productivity
- Downtime
- Environmental Penalty

Results in $ and MW/MWh.

Physical Security Model — A First for Data Centers

PHASE 1 —

Physical-to-Cyber

Physical outsider bypasses perimeter controls to reach ICS/OT assets and launch a cyber attack from inside the security boundary. Delay / Detection / Response modeled.

PHASE 2 —

Physical-to-Physical

Physical outsider bypasses controls to directly vandalize or destroy critical infrastructure — servers, cooling, power systems. Primary driver of Equipment Damage.

Total Expected Loss — Cyber & Physical Combined

MEAN ANNUAL EXPECTED LOSS

$4.77 MM

1 hyperscale facility · 150MW · US · annual model · DeRISK CRQ v5.x with Physical Security Zones v2.0

CYBER $3.09MM (64.8%)

PHYSICAL $1.68MM (35.2%)

VaR 95th · 1-in-20 year loss	VaR 97th · 1-in-33 year loss	VaR 99th · 1-in-100 year loss
$17.2MM	**$21.9MM**	**$27.9MM**

■ KEY INSIGHT

35% of expected annual loss originates from physical attack paths — not network intrusion.

Physical security investment has, for the first time, a quantified ROI in financial risk terms.

CAPACITY AT RISK — MW IMPACT TIERS (150MW FACILITY)

FULL	HIGH	MEDIUM	LOW
150MW	**120MW**	**30MW**	**7.5MW**
100% capacity	80% capacity	20% capacity	5% capacity
All buildings	Multiple buildings	1 building / multi-hall	1 data hall / fault domain

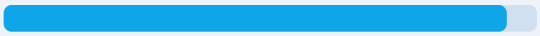
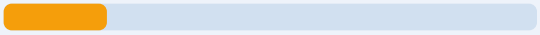
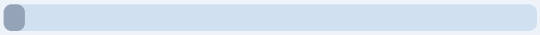
FACILITY CONTEXT

Scope:	1 hyperscale data center facility, US
Framework:	NIST CSF — OT security posture assessment
Data:	Customer-provided OT telemetry: asset inventory, vulnerability data, network topology
Data period:	Annual expected loss — modeled output, June 2025

What does the $4.77MM consist of?

DeRISK CRQ decomposes expected annual loss into primary and secondary loss events.

MEAN EXPECTED LOSS PER LOSS EVENT · $ AND MW/MWH WHERE APPLICABLE

	MEAN EL →	MEAN	VaR 95%	VaR 99%
Equipment Damage (56.6%)		$2.70MM	$14.0MM	$26.5MM
Extortion (25.3%)		$1.20MM	$14.9MM	$23.9MM
Loss of Productivity (11.6%, ≥7.5MW affected)		$554K	$1.94MM	$10.8MM
Downtime (3.3%, MW/MWh output)		$159K	$777K	$1.40MM
Environmental Penalty (2.4%)		$114K	$1.08MM	$2.37MM
Other (0.5%)		$23K	—	—
Total Mean Expected Loss		**$4.77MM**	$17.2MM	$27.9MM

Equipment Damage is the #1 loss driver at 56.6% of mean expected loss.

Driven by both cyber-to-physical (OT system compromise → equipment failure) and physical-to-physical (outsider bypass → direct sabotage).

■ **MW/MWh output: Full = 150MW · High = 120MW · Medium = 30MW · Low = 7.5MW (see results page for full tier breakdown)**

The 35% That Changes the Conversation

For this operator, more than one-third of annual expected loss traces directly to physical attack paths — not network intrusion. This insight was only possible because DeRISK CRQ modeled both attack surfaces in a single probabilistic framework.

PHASE 1 — PHYSICAL-TO-CYBER

Outsider → Cyber Attack

Physical outsider bypasses perimeter barriers, access controls, and CCTV to reach ICS/OT assets inside the facility.

Attacker launches cyber attack targeting BMS, EPMS, PACS, or DCIM from within the trusted security zone.

DeRISK models: delay, detection, guard presence, response time across all physical security zones.

Contributes to: Equipment Damage, Downtime, Loss of Productivity, Extortion.

PHASE 2 — PHYSICAL-TO-PHYSICAL

Outsider → Direct Damage

Physical outsider bypasses controls to directly vandalize, sabotage, or destroy critical physical infrastructure:

· Server and compute equipment
· Cooling and HVAC systems
· Power distribution and UPS
· Battery and generator backup

Drives Equipment Damage — #1 loss event at 56.6% of mean expected loss ($2.70MM).

No network intrusion required.

PHYSICAL ZONE HIERARCHY — ATTACK PATH DIRECTION

Public Access – Perimeter Zone – Facility Entrance – Operations Floor – Critical Zone (ICS/OT)

PHYSICAL SECURITY CONTROLS MODELED IN DERISK

Delay Capabilities

Physical barriers · Access control systems · Fences and gates

Detection Capabilities

Access point monitoring · CCTV coverage · Guard presence · Video review intervals

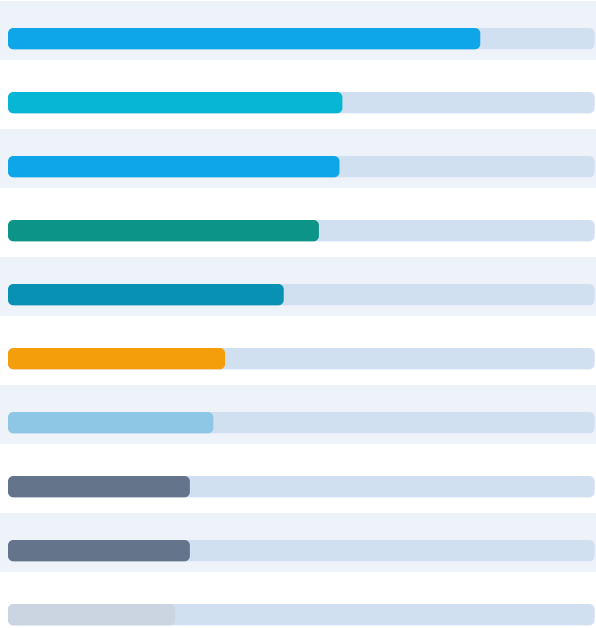
Response Capabilities

Emergency response time · Coordination with security operations center

What is driving cyber expected loss — and why?

DeRISK CRQ attributes cyber expected loss ($3.09MM) to Initial Access Vectors (IAVs) — the methods attackers use to first breach a facility. IAV proportions are calibrated annually using multi-source threat intelligence (Mandiant, IBM X-Force, Kaspersky, Cyentia) and adjusted for facility-specific exposure signals.

EXPECTED LOSS BY INITIAL ACCESS VECTOR (CYBER ONLY — $3.09MM TOTAL)



Exploit Public-Facing Application	16.1%	**$496.9K**
Spearphishing	11.4%	**$352.9K**
Valid Accounts	11.3%	**$347.4K**
External Remote Services	10.6%	**$328.5K**
Remote Services	9.4%	**$289.9K**
Phishing	7.4%	**$227.1K**
Supply Chain Compromise	7.0%	**$216.7K**
Transient Cyber Asset	6.2%	**$191.6K**
Exploitation of Remote Services	6.2%	**$191.3K**
Drive-by Compromise	5.7%	**$177.0K**
Total Cyber Mean Expected Loss		**$3.09MM**

Why does Phishing appear in a facility with isolated OT networks?

Even when OT networks have no direct internet connectivity, enterprise-side credential exposure creates indirect access risk. DeRISK detected leaked employee credentials for this operator — elevating Phishing above the 46% industry baseline.

IAV proportions calibrated from: Mandiant M-Trends 2025, IBM X-Force 2025, Kaspersky IR 2024, Cyentia IRIS.

Facility-specific adjustments applied for externally visible CVEs, open ports, and leaked credential score. Enterprise and ICS MITRE ATT&CK matrices applied.

Mitigate · Transfer · Accept

With quantified risk in hand, the operator can take structured action across three dimensions — backed by financial evidence, not just technical findings.

MITIGATE

Buy down risk through targeted controls

- **Top priority — EPFA**
  Exploit Public-Facing Application drives $497K mean EL. Patch exposed services, harden internet-facing infrastructure, review firewall rules.
- **Physical security ROI**
  Phase 1 and Phase 2 controls contribute $1.68MM in physical EL. Every additional delay layer reduces attack path success probability.
- **Credential hygiene**
  Leaked credentials elevated Phishing IAV above industry baseline. Implement MFA, credential rotation, and dark web monitoring.

TRANSFER

Optimize cyber insurance coverage

- **Quantified exposure for brokers**
  Mean EL $4.77MM and VaR 99th $27.9MM provide actuarially-grounded data brokers and underwriters need to structure coverage correctly.
- **Equipment Damage focus**
  $2.70MM mean EL from equipment damage — the largest single category — directly informs property/cyber insurance coverage limits.
- **Physical security recognized**
  DeRISK output documents physical controls as compensating controls, supporting premium negotiation with cyber insurers.

ACCEPT

Reserve for residual risk

- **Know your liability**
  Mean EL $4.77MM is the annual reserve figure — the dollar amount carried on the balance sheet as cyber + physical risk.
- **Board-level reporting**
  VaR at 95th/97th/99th percentile gives the board a clear risk tolerance framework in financial risk governance language.
- **Portfolio context**
  Per-facility EL enables portfolio roll-up: which sites carry the most exposure, and where does marginal risk reduction have highest impact?

THE BIGGER PICTURE

From one facility to a portfolio-level risk management program.

This engagement covers a single 150MW facility. The operator runs dozens of hyperscale data centers across North America and beyond. DeRISK CRQ scales across the full portfolio — generating per-facility EL/VaR, portfolio accumulation analysis (CoEXP module), and a unified financial risk view that connects OT security posture to board-level capital allocation decisions.

Physical security modeling — quantified and comparable across sites — becomes a competitive differentiator in insurance and risk transfer.

Why data centers are uniquely well-suited for DeRISK CRQ

Hyperscale and large data centers share structural characteristics that make quantified cyber risk especially powerful — and especially actionable.

DERISK CRQ — DATA CENTER CAPABILITY MAP

OT Systems in Scope:	BMS, EPMS, PACS, DCIM, Air Handling, Water Handling, Battery & Generator Backup
Financial Model:	Loss expressed in $ and MW/MWh — revenue loss per hour, capacity at risk, equipment damage
Physical Security:	Phase 1 (physical-to-cyber) + Phase 2 (physical-to-physical) — quantifies perimeter value in $
Attack Surface:	External CVEs, open ports, leaked credentials — continuously refreshed outside-in data
Inside Data:	Customer-provided OT telemetry: asset inventory, vulnerability data, network topology
Frameworks:	NIST CSF 1.1 · ISO 27001 · DNX CSF (23 OT-native controls) — all three supported
Portfolio:	Per-facility EL/VaR + portfolio accumulation via CoEXP module — scales to 100s of sites
Reporting:	Executive dashboard, board-ready EL/VaR reports, compliance overview, insurance data package

Budget Justification

Translate OT security investment into ROI. Show the board the dollar reduction in expected loss per control project — cyber and physical combined.

Cyber Insurance

Provide underwriters with quantified, OT-specific exposure data — EL, VaR, loss event breakdown, MW at risk — to optimize coverage and negotiate premiums.

Board & Exec Reporting

On-demand reports in financial language, not vulnerability counts. VaR figures, loss attribution, and cyber/physical risk trend over time.

Ready to quantify your data center cyber and physical risk?

Contact DeNexus to discuss your portfolio. Results delivered in weeks, not months.

denexus.io

GLOSSARY OF TERMS

Key terms used in this case study

APA
Attack Path Algorithm — DeRISK module estimating probability of a successful attack reaching a loss event, given facility security controls and network topology.

CoEXP
Co-Exposure Module — DeRISK module for portfolio-level risk accumulation. Models correlated losses across multiple facilities.

CRQ
Cyber Risk Quantification — expressing cyber risk exposure in financial terms (dollars), enabling business-level risk decisions.

EL / Expected Loss
Mean Annual Expected Loss — the average dollar loss the facility can expect per year, used for reserving and budgeting.

IAV
Initial Access Vector — the method by which an attacker first gains access to a target. DeRISK models 19 IAVs mapped to MITRE ATT&CK.

ICS/OT
Industrial Control Systems / Operational Technology — hardware and software managing physical processes in a data center (power, cooling, access, infrastructure management).

LEI
Loss Event Impact — DeRISK module translating a successful attack into dollar values: Equipment Damage, Extortion, Downtime, Loss of Productivity, Environmental Penalty.

MITRE ATT&CK
Globally-accessible knowledge base of adversary tactics, techniques, and procedures. DeRISK uses both Enterprise and ICS matrices.

MW / MWh
Megawatt / Megawatt-hour — units of capacity and energy. DeRISK expresses Downtime and Loss of Productivity in both $ and MW/MWh for data center operators.

NoA
Number of Attack Attempts — DeRISK module estimating how many attacks a facility will experience per year, per IAV, using firmographics and outside-in data.

NIST CSF
National Institute of Standards and Technology Cybersecurity Framework — 108 controls across Identify, Protect, Detect, Respond, Recover.

Physical Security Model
DeRISK capability modeling physical outsider attack paths alongside network-based cyber attacks. Phase 1 = physical-to-cyber; Phase 2 = physical-to-physical.

URMS
Unit Risk Modeling System — the core DeRISK engine combining NoA, APA, and LEI to produce per-facility Expected Loss and Value at Risk.

VaR
Value at Risk — maximum expected loss at a given confidence level. VaR 99th ($27.9MM) = the loss level exceeded only 1% of the time in a given year.