DENEXUS™

AUGUST 2026 | NEWSLETTER

OT CYBER RISK INTELLIGENCE NEWSLETTER

• Quantify • Reduce • Transfer

Thought leadership on underwriting-grade OT evidence, AI-driven vulnerability discovery, and the DeRISK platform for quantifying and reducing cyber risk.

denexus.io

CONTENTS

01 **Explainable Quantification** p. 3

No audit trail, no decision-grade number

02 **OT Attacks & Industry News** p. 6

Minnesota water systems, Coca-Cola ransomware, GOLD EAGLE, CISA advisories

03 **DeNexus News** p. 9

Events, webinars, research reports, and upcoming panel

04 **DeRISK Platform** p. 11

Quantify, Reduce, Transfer - Complete solution overview

Thought Leadership

Explainable quantification: no audit trail, no decision-grade number

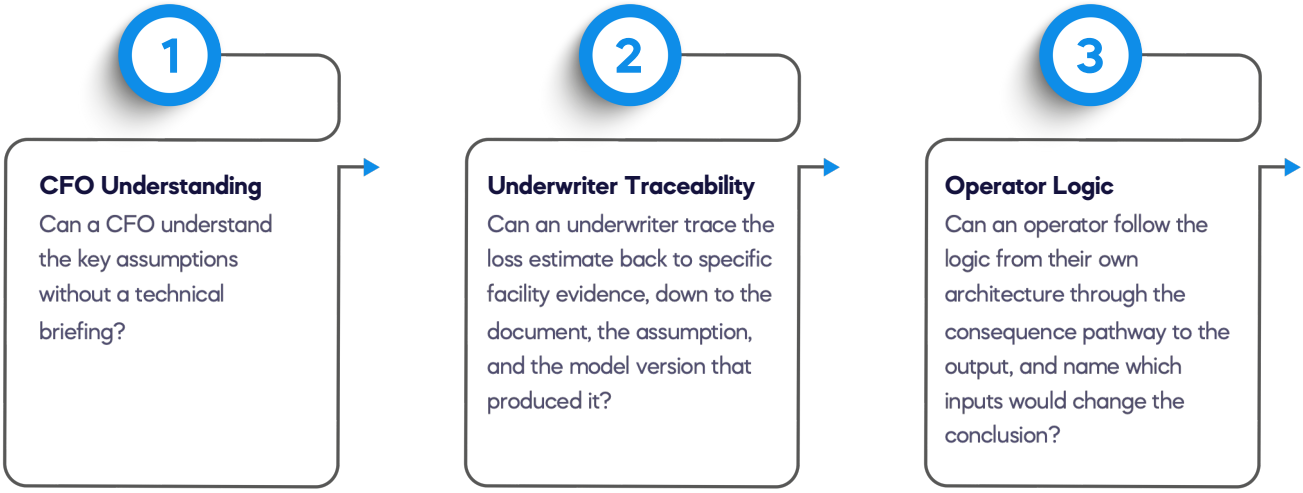
The operating model for cyber-physical risk management with traceability standards

Thought Leadership

Explainable quantification: no audit trail, no decision-grade number

Quantification only works when it's explainable. Engineers must be able to trace the logic from facility evidence to the loss estimate. Markets must be able to audit the evidence and assumptions without asking the insured to interpret them. CFOs must be able to defend the number to a board without retreating into assertions about model complexity.

The test is direct, and it has three parts.



If any answer is no, the number isn't ready. It is a calculation, not a governance artifact.

The gap shows up most sharply in restoration economics, because restoration is where loss actually accumulates. When Norsk Hydro was hit by LockerGoga ransomware in 2019, the company put the cost at roughly $70 million, and the bulk of it wasn't destroyed equipment. It was weeks of aluminum production running in degraded manual mode while systems were rebuilt. A loss estimate that models direct damage precisely but bounds restoration duration with an unexplained assumption has quantified the small component and guessed at the large one. Every reviewer who checks the work will find that guess.

The discipline this month is converting opaque quantification into traceable quantification. Opaque means benchmark averages, black-box scoring, or correlation assumptions nobody can locate. Traceable requires three things: facility-level inputs that are auditable, scenarios that are versioned with explicit feasibility conditions, and assumptions that carry a date stamp and a methodology reference. Build those three and the number can be challenged, updated, and defended. Skip them and the number is at risk of dismissal at exactly the moment it matters most.

WHAT MATTERS THIS MONTH

Facility is the exposure unit; portfolio is the priced object.

Aggregation is a distribution problem, not an averaging problem. Two portfolios with identical mean loss can carry radically different tails, and the tail (VaR, TVaR) is what drives the capital conversation. Averaging facility estimates destroys the information that pricing needs.

Loss components must be evidenced, and restoration drivers are central

Direct damage estimates paired with unbounded restoration timelines aren't credible loss estimates. The evidence that bounds duration is specific: tested restore procedures with timestamps, dependency maps for long-lead equipment, documented manual-operation capacity. Norsk Hydro could run degraded because operators still knew manual mode; your estimate should state whether yours do.

Traceability is mandatory, not aspirational.

Evidence to assumptions to outputs, versioned and reviewable. A number you can't reproduce is a number you can't defend, and a number that can't be defended won't earn the terms it should.

WHAT YOU CAN DO NOW

Build a one-page traceability chain for each critical site.

This scenario, these assumptions, this evidence, this output. Where any link is missing, the chain breaks, and so does the defensibility of the result. One page per site is enough; the constraint forces clarity.

Make sensitivity explicit.

Name the three to five assumptions that move the answer materially. Restoration duration, scenario feasibility, and dependency constraints usually top the list. Disclose them rather than burying them in model complexity. Sensitivity disclosure is the hallmark of governance-grade quantification, and it's also the fastest way to focus the next round of evidence collection.

For market-facing discussions, keep models bounded and auditable rather than opaque and complex.

Complexity isn't rigor. Auditability is. An underwriter who can follow your logic in an afternoon prices with more confidence than one handed a thicker model they can't open.

Next month

Reduce and validate: controls that measurably change the loss curve.

Educational content only. Not legal, coverage, or underwriting advice.

Industry News

OT Attacks, Regulation & Insurance Developments

CISA BOD 26-04, Check Point VPN, UK NCSC threats, and cyber insurance market updates

Industry News

OT CYBER ATTACKS & INCIDENTS

Seven states, one method: what the public record now confirms about the water-sector attacks

A joint FBI/EPA advisory on 30 July confirmed that water and wastewater utilities in at least seven states reported incidents from 27 July, using a documented method: remote access to internet-facing Rockwell MicroLogix PLCs, then IP and password changes that locked operators out. Reported effects included pressure loss, flooding, and boil-water notices — but no drinking-water contamination anywhere. Attribution isn't settled: investigators call Iranian involvement probable, while Minnesota says the determination is the federal government's to make. The durable lesson sits underneath that question — the FBI names four factors that decided how far each incident went, and one is simply whether the utility could still run its process manually. That's an engineering property: specifiable, testable, and evidenced, no matter who was responsible.

Read the full dated record from DeNexus CEO, José M. Seara — seven states, the confirmed method, and why attribution isn't settled →

→ **Read More**

Coca-Cola's fairlife ransomware event caused a temporary U.S. production halt.

Coca-Cola disclosed that fairlife identified unauthorized third-party access to part of its systems, including production-related systems, in connection with a ransomware event [1]. The company activated incident response and business-continuity protocols, said product quality and safety were not impacted, but temporarily suspended fairlife production operations in the United States while Canadian production was not affected [1], [2]. Reuters later reported that fairlife had resumed most production at four U.S. facilities and that Coca-Cola did not expect the incident to have a material impact on financial condition or results [3]. This is not a confirmed OT compromise, but it is a clear food-and-beverage business-interruption story where cyber affected production-related systems and physical output.

REGULATION & POLICY DEVELOPMENTS

White House launches GOLD EAGLE to coordinate AI-era vulnerability remediation.

The White House announced GOLD EAGLE on July 14 as a public-private clearinghouse for cybersecurity vulnerability coordination, linking federal partners, open-source software partners, critical infrastructure companies, and industry participants [4]. The stated objective is to use frontier AI capabilities to reduce duplicative scanning, intake and prioritize identified vulnerabilities, coordinate scanning verification, and deliver actionable remediation information to defenders. For OT and critical-infrastructure operators, the significance is not that GOLD EAGLE solves vulnerability management; it is that government is acknowledging a new operating reality: AI-assisted discovery can increase vulnerability volume and speed, so remediation coordination must become faster, more prioritized, and more connected to criticality.

OT SECURITY GUIDANCE

CISA's updated PLC advisory moves the warning from single-vendor exposure to broader PLC hardening.

The July 22 update to joint advisory AA26-097A adds guidance for detecting malicious changes in reusable code modules within Rockwell Automation PLC programs and expands observed targeting to Schneider Electric, Siemens, and potentially other PLC manufacturers [5]. The agencies report targeting of internet-connected OT devices, including PLCs, with malicious project-file interaction, HMI/SCADA data manipulation, and in some cases operational disruption and financial loss. The practical guidance is direct: remove PLCs from public internet exposure, query logs for IOCs and suspicious traffic on OT ports such as 44818, 2222, 102, and 502, restrict access through secure gateways, validate project files and reusable logic, secure cellular modems, use MFA and strong access control, and maintain known-good offline backups. For industrial operators, this is a reminder that "remote access" cannot mean exposed controllers; every path into a PLC should be mediated, monitored, authenticated, and recoverable.

CYBER INSURANCE & RISK TRANSFER

Marsh reports continued cyber-rate softening, but risk quality still matters.

Marsh's Q2 2026 Global Insurance Market Index reported that global commercial insurance rates fell 6% in the quarter, the eighth consecutive quarterly decline, while cyber insurance rates fell 4%, the twelfth consecutive quarterly decline [6]. Marsh attributed the softer market to strong insurer competition, stable capacity, favorable reinsurance conditions, surplus capital, and stronger insurer financial performance, and noted that broader coverage, higher limits, and reduced retentions were often available. For industrial buyers, this creates a useful window to revisit limits, retentions, captives, cyber-physical wording, and program structure, but not a reason to treat underwriting evidence as optional. Marsh still notes that outcomes vary by risk quality, exposure management, and program structure, which is exactly where quantified OT scenarios and recoverability evidence can improve placement results.

WORKS CITED

[1] The Coca-Cola Company. "The Coca-Cola Company Announces Technology Disruption Involving fairlife Operations." The Coca-Cola Company Investor Relations, 16 July 2026, https://investors.coca-colacompany.com/news-events/press-releases/detail/1166/the-coca-cola-company-announces-technology-disruption-involving-fairlife-operations

[2] The Coca-Cola Company. "Form 8-K." U.S. Securities and Exchange Commission, 16 July 2026, https://www.sec.gov/Archives/edgar/data/21344/000162828026048466/ko-20260716.htm

[3] Reuters. "Coca-Cola Says fairlife Resumes Production at 4 US Plants after Cyberattack." Reuters, 27 July 2026, https://www.reuters.com/business/coca-cola-says-fairlife-resumes-production-4-us-plants-2026-07-27/

[4] The White House. "White House Launches Gold Eagle Initiative for Unprecedented Cybersecurity Vulnerability Coordination." The White House, 14 July 2026, https://www.whitehouse.gov/releases/2026/07/white-house-launches-gold-eagle-initiative-for-unprecedented-cybersecurity-vulnerability-coordination/

[5] Federal Bureau of Investigation, Cybersecurity and Infrastructure Security Agency, National Security Agency, Environmental Protection Agency, Department of Energy, U.S. Cyber Command Cyber National Mission Force, and Department of the Treasury. "Iranian-Affiliated Cyber Actors Exploit Programmable Logic Controllers across US Critical Infrastructure." IC3 / Joint Cybersecurity Advisory AA26-097A, updated 22 July 2026, https://www.ic3.gov/CSA/2026/260722.pdf

[6] Marsh. "Global Insurance Market Index." Marsh, Q2 2026, https://www.marsh.com/en/services/international-placement-services/insights/global-insurance-market-index.html

Industry News

03

Events, Webinars & Research Reports

Where you'll find us this month and the latest insights from DeNexus

Upcoming Event

ISA / ISASecure Webinar

José María Seara, Founder & CEO, DeNexus

Topic: OT Cyber Insurance & Risk Transfer: Right-Sizing Coverage Using Evidence, Not Guesswork

Date: Wednesday, September 9, 2026

Time: 11:00 AM – 12:00 PM EDT

Fortinet Toronto OT Leadership Day

José María Seara, Founder & CEO, DeNexus

Date: Wednesday, September 23, 2026

Time: 11:00 AM – 12:00 PM EDT

Upcoming Webinars

DeRISK UWA — Underwriting OT Cyber Risk, End to End

A live session with Chaucer on DeRISK UWA — how five specialist AI agents take an underwriter from raw submission to a full actuarial assessment in 10–20 minutes, and where the human decision stays in control.

30 minutes | Guest session + live Q&A | September 9, 2026

DeRISK CRQ & QVM — Building a Multi-Year Risk Reduction Program

How DeRISK CRQ and QVM turn OT cyber exposure into financial terms — Expected Annual Loss and Value at Risk — then drive a multi-year reduction program: a measured baseline, fixes ranked by expected loss reduction, and quarterly reviews the risk committee can act on.

30 minutes | Guest session + live Q&A | September 16, 2026

The DeNexus Learning Hub is live.

One place for the foundational material on OT cyber risk in financial terms: the OT Cyber Risk Knowledge Center, practitioner-level articles and guides across quantification, controls, and risk transfer, direct answers to the questions boards and CISOs ask most often, and reference tools for operationalizing a risk program. Whether you're building the business case internally or briefing a risk committee, it's designed to be the starting point.

→ **Explore The Learning Hub**

Research Reports — Live & In the Works

H1 Manufacturing Report
→ Download Report

US AI Data Center Report
→ Download Report

Lender's Resource Kit
→ Download Report

Iran War & Industrial OT Risk
Coming September 2026

Edge Models & Industrial Cyber Risk
Coming September 2026

The DeRISK Platform — Quantify and Reduce

DeRISK Platform Overview

One simulation core for two critical functions: Quantify and Reduce

The DeRISK Platform covers two of the three moves in the model — **Quantify** and **Reduce** — through CRQ and QVM, built on one simulation core. One quantifies risk in dollars; together they tell you which work removes the most of it.

DeRISK CRQ

Cyber Risk Quantification

DeRISK QVM

Quantified Vulnerability Management

DeRISK UWA Agentic

Agentic Underwriting

DeRISK CRQ — Quantify

Cyber Risk Quantification translates OT exposure into Expected Annual Loss and Value at Risk, then simulates which controls and projects reduce that loss the most per dollar spent — at the facility and across the portfolio. It gives CISOs, CFOs, and boards a defensible financial view of risk instead of a red-amber-green dashboard, and reframes the cyber conversation as a capital allocation conversation.

- Translates OT exposure into financial loss
- Simulates control effectiveness
- Portfolio-level analysis

DeRISK QVM — Reduce

Quantified Vulnerability Management ranks every CVE by expected loss reduction, not by CVSS score. CVEs are matched to your asset inventory and network context, cross-referenced against active NVD and CISA advisories, mapped to MITRE ATT&CK for Enterprise and ICS through a patent-pending AI pipeline, and run through a simulation-twin of your network that computes the financial loss each vulnerability contributes. The result surfaces the 1–2% of vulnerabilities that drive roughly 90% of real risk — and lets you simulate remediation before committing an outage window.

- Ranks by expected loss reduction
- Cross-references NVD advisories
- Simulates remediation before outage

Ready to see the DeRISK Platform in action?

Schedule a demo with our team to see how DeRISK can transform your OT cybersecurity strategy.

Book a Demo →

DeRISK UWA Agentic — Transfer

AI-native underwriting platform for the cyber insurance market

DeRISK UWA Agentic completes the Quantify – Reduce – Transfer model. Our AI-native underwriting platform for the cyber insurance market — underwriters, MGAs, and Lloyd's syndicates writing industrial and OT risk — launched in May, entering early-adopter deployment with Chaucer Group as the named reference.

Underwriting OT exposure has always been hard — limited evidence, inconsistent submissions, and not enough specialist capacity to assess every risk in depth. DeRISK UWA Agentic closes that gap. Its agentic workflow moves from submission ingestion to actuarial output in minutes — expected loss, maximum foreseeable loss, full loss exceedance curves, premium indication, and a structured insurance program — with every finding traceable to its source document, pipeline step, and model version.

Agentic Workflow

Moves from submission ingestion to actuarial output in minutes: expected loss, maximum foreseeable loss, full loss exceedance curves, premium indication, and a structured insurance program.

Traceability

Every finding traceable to its source document, pipeline step, and model version. Evidence that cannot be traced cannot be audited.

Augment your underwriting team — without hiring.

→ Learn More