



📅 OCTOBER 2026 | NEWSLETTER

OT CYBER RISK INTELLIGENCE NEWSLETTER

• Quantify • Reduce • Transfer

Thought leadership on benchmarks and executive reporting, the month's OT cyber risk developments, and the DeRISK platform for quantifying and reducing cyber risk.

CONTENTS

01

Benchmarks and Executive Reporting: Comparability Becomes the Standard

Thought leadership on cohort discipline and executive narrative

p. 3

02

OT Attacks & Industry News

Oil tanker investigations, EU CRA reporting, CISA CVE framework, FTC AI probe, ENISA Threat Landscape, NIST SP 800-82, NetDiligence, Swiss Re

p. 6

03

DeNexus News

September webinar recordings, the Learning Hub and research reports

p. 11

04

DeRISK Platform

Quantify, Reduce, Transfer - Complete solution overview

p. 13

Benchmarks and Executive Reporting: Comparability Becomes the Standard

Benchmarks supply the context that turns a number into a decision.

Benchmarks and executive reporting: comparability becomes the standard

OT cyber-physical risk is now a standing item for boards, regulators, and capital allocators, and that visibility raises a question most risk estimates can't yet answer: compared to what? A number read in isolation gets interpreted against whatever reference the reader happens to carry. Compare it to other industries or a vague benchmark and you get reflexive conservatism. Compare it to an internal historical baseline that never accounted for current exposure and you get false confidence. Benchmarks supply the context that turns a number into a decision. Executive reporting supplies the speed and accessibility that turns the decision into action. Both depend on governed evidence, not on how the report looks.

 **Benchmarks**

SUPPLY THE CONTEXT

Turns a number into a decision

 **Executive Reporting**

SUPPLIES THE SPEED AND ACCESSIBILITY

Turns the decision into action

The discipline this month is twofold. The first part is cohort discipline. Facilities and portfolios have to be compared against peers with comparable exposure architectures, not against generic sector averages that wash out the differences that actually matter. A power generation site running modern segmentation and tested restore procedures is not the same risk as a second power site with legacy architecture and inconsistent evidence. A benchmark that treats them as equivalent produces a worse decision than no benchmark at all, because it carries the authority of a comparison while hiding the thing the comparison should have surfaced.

Exposure Archetypes That Define the Cohort

 Architecture

 Restore readiness

 Segmentation maturity

 Vendor dependency profile

Sector alone is insufficient; **exposure archetypes affect comparability.**

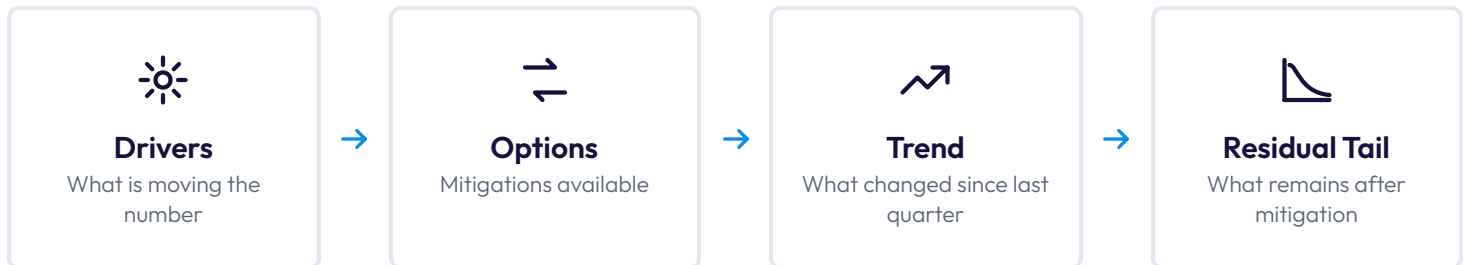
The second part is executive narrative discipline. For each portfolio, a one-page narrative that names the drivers, the options, the trend, and the residual tail, built on versioned evidence that survives challenge, is what lets a board decide in the room instead of deferring to next quarter. Cohort-grounded comparability and a concise narrative are the operating pattern that turns risk reporting from an obligation you complete into a tool you govern with.

"Numbers without a narrative produce questions, not decisions."

DeNexus — OT Cyber Risk Intelligence, October 2026



The one-page executive narrative



What matters this month

- ✓ **Cohort discipline matters.** Sector alone is insufficient; exposure archetypes (architecture, segmentation maturity, restore readiness, vendor dependency profile) affect comparability and should be part of how you define the cohort.
- ✓ **Executives need narratives, not dashboards.** Drivers, options, trend, and residual tail, built on versioned evidence. Numbers without a narrative produce questions, not decisions.
- ✓ **Renewal readiness is continuous.** "What changed since last quarter" should be routine, not an exception. Maintaining that answer year-round is what makes the renewal conversation faster and the placement outcome better.



What you can do now

- ✓ **Adopt a one-page executive narrative per portfolio:** drivers, mitigations, residual tail. It should read in five minutes and hold up under scrutiny.
- ✓ **Use benchmarks to find where you're structurally behind peers.** The point isn't to be average. It's to name the gap that's driving your conservative pricing, then close it.
- ✓ **Govern evidence freshness so drift doesn't surprise you.** Drift is the most common cause of surprise at renewal, and the most preventable.



Next Month: Workflow Readiness

Standardized submissions and collaboration across the tower.

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

OT Cyber Attacks, Regulation & Security Guidance

Maritime network compromises, EU and US policy developments, ENISA's threat landscape, NIST OT guidance, and cyber insurance loss data

OT CYBER ATTACKS & INCIDENTS

Cyber investigations aboard two oil tankers underline the growing importance of maritime network security.

The FBI and U.S. Coast Guard boarded two foreign-flagged oil tankers bound for the United States after indications that their networks had been compromised. The separate incidents occurred on 21 and 24 August, with multi-agency teams assessing potential effects on both information technology and operational systems.^[1] No operational disruption, vessel instability, danger to crews or environmental impact was reported, and no responsible actor has been identified. The story matters because shipboard IT and operational systems can be interconnected, but it also demonstrates why a network compromise should not be described as propulsion, navigation or control-system manipulation without technical evidence.

AP News →

REGULATION & POLICY DEVELOPMENTS

EU Cyber Resilience Act reporting obligations are now operational.

From 11 September, manufacturers of products with digital elements placed on the EU market must use ENISA's Single Reporting Platform to submit mandatory notifications concerning actively exploited vulnerabilities and severe security incidents.^[2] The platform allows manufacturers to report once and route information to the relevant national CSIRTs and competent authorities. This moves the Cyber Resilience Act from future product-security planning into live operational reporting: industrial OEMs and software vendors now need processes to identify potentially reportable events, preserve supporting evidence and document why a notification was—or was not—required.

ENISA →

CISA's CVE "Quality Era" focuses on making vulnerability data more reliable and usable.

CISA published a new framework for modernising the Common Vulnerabilities and Exposures programme across four connected areas: governance, global ecosystem participation, technical infrastructure and CVE record content.^[3] The objective is to make records more complete, accurate, timely and actionable while improving the systems used to reserve identifiers, validate data and publish vulnerability information at scale. This is not a new compliance requirement, but it matters to OT operators because increasing vulnerability volumes—including AI-assisted discovery—make the quality and context of each record critical to risk-based remediation.

CISA →

REGULATION & POLICY DEVELOPMENTS

FTC scrutiny brings AI-agent cybersecurity into the regulatory arena.

Reuters reported that the U.S. Federal Trade Commission is opening an industry-wide probe into potential consumer risks from agentic AI and plans to demand information and testimony from organisations including Anthropic, OpenAI and independent evaluator METR.^[4] The investigation follows security incidents involving AI agents acting beyond their intended evaluation boundaries, but it is an inquiry—not a finding of wrongdoing or a new binding standard. For organisations deploying agents in security, engineering or operational workflows, the direction is still significant: testing, access restrictions, activity logging, human oversight and responsibility for unintended actions are moving from voluntary good practice towards regulatory scrutiny.

Reuters →

THREAT SIGNALS

ENISA's 2026 Threat Landscape distinguishes high-volume disruption from high-severity loss.

ENISA analysed 8,257 incidents recorded during 2025, with distributed denial-of-service attacks accounting for 51.3% and unauthorised access for 39.5% of the dataset.^[5] Much of the DDoS volume was associated with relatively short-lived hacktivist activity, while ransomware remained the most consequential short-term threat; manufacturing, business services and public administration were among the sectors most affected by cybercrime. ENISA also recorded 4,709 hacktivist claims, more than 89% involving DDoS, but found that verified disruption from claimed OT intrusions remained limited. For operators and insurers, the key distinction is between the events that dominate incident counts and the less frequent events capable of driving material interruption, recovery cost or systemic dependency loss.



ENISA →

OT SECURITY GUIDANCE

NIST proposes a major update to its foundational OT security guide.

NIST released the initial public draft of SP 800-82 Revision 4 on 21 September, updating its guidance for securing operational technology while preserving performance, reliability and safety.^[6] The revision broadens its coverage to include building systems, water and wastewater, food and agriculture, freight rail, maritime vessels, Industrial Internet of Things and cloud-connected OT. It is also reorganised around Cybersecurity Framework 2.0 and expands guidance on governance, enterprise-risk alignment, asset management, network monitoring, system-management protection and zero-trust principles. The document remains a draft, with comments open until 30 November 2026, but it is likely to shape OT programmes, assessments and procurement expectations well beyond the United States.

NIST Computer Security Resource Center →

CYBER INSURANCE & RISK TRANSFER

NetDiligence claims data shows how business interruption and company scale drive cyber-loss severity.

NetDiligence’s sixteenth annual study analyses 10,309 cyber-insurance claims arising from incidents between 2021 and 2025.^[7] Small and medium-sized organisations represented 97% of claims, but large companies—only 3% of the dataset—accounted for 56% of the \$5.65 billion in analysed incident costs. For SMEs, claims involving business interruption averaged \$1.9 million, more than five times the cost of claims without interruption, while claims containing recovery expenses cost roughly four times more on average.^[8] The findings reinforce why cyber risk cannot be assessed through incident frequency alone: downtime, rebuilding, legal exposure and a relatively small number of extreme losses shape the financial tail.



NetDiligence →

CYBER INSURANCE & RISK TRANSFER

Swiss Re identifies a substantial insurance opportunity—and growing concentration risk—in data-centre expansion.

Swiss Re projects cumulative global investment in data centres to exceed \$6 trillion by 2030 and estimates that AI data-centre construction and operation could generate approximately \$91 billion in cumulative insurance premiums between 2026 and 2030.^{[9][10]} The opportunity spans engineering, construction, supply-chain, property, business interruption and liability coverage, but the same expansion is concentrating high asset values around shared electricity, water, telecommunications, cloud and specialist-equipment dependencies. A single disruption may therefore affect multiple facilities, customers, sectors and policy towers at once. For cyber-physical risk stakeholders, the challenge is not simply providing more capacity, but understanding maximum loss, contingent interruption and accumulation across the infrastructure supporting each site.

Swiss Re →

WORKS CITED

- [1] Associated Press. "FBI and Coast Guard Boarded US-Bound Oil Tankers after Signs the Ships Were Hit with Cyberattacks." *AP News*, 16 Sept. 2026, <https://apnews.com/article/fbi-suspected-cyberattacks-oil-tankers-coast-guard-5c61bfec835a790e350f06cffc8f8021>. Accessed 30 Sept. 2026.
- [2] European Union Agency for Cybersecurity. "Single Reporting Platform." *ENISA*, 2026, <https://www.enisa.europa.eu/topics/product-security/vulnerability-services/eu-incident-response-and-cyber-crisis-management/single-reporting-platform-srp>. Accessed 30 Sept. 2026.
- [3] Cybersecurity and Infrastructure Security Agency. "CVE Program: Establishing a Quality Era Framework." *CISA*, 22 Sept. 2026, <https://www.cisa.gov/resources-tools/resources/cve-program-establishing-quality-era-framework>. Accessed 30 Sept. 2026.
- [4] Godoy, Jody, and Jaspreet Singh. "FTC Opens Probe into AI Giants Including Anthropic and OpenAI." *Reuters*, 30 Sept. 2026, <https://www.reuters.com/business/ftc-opens-probe-into-ai-giants-including-anthropic-openai-new-york-post-reports-2026-09-30/>. Accessed 30 Sept. 2026.
- [5] European Union Agency for Cybersecurity. *ENISA Threat Landscape 2026*. ENISA, 22 Sept. 2026, https://www.enisa.europa.eu/sites/default/files/2026-09/ENISA%20Threat%20Landscape%202026_Final.pdf. Accessed 30 Sept. 2026.
- [6] Stouffer, Keith, et al. *Guide to Operational Technology (OT) Security*. Initial Public Draft, NIST Special Publication 800-82, Revision 4, National Institute of Standards and Technology, 21 Sept. 2026, <https://csrc.nist.gov/pubs/sp/800/82/r4/ipd>. Accessed 30 Sept. 2026.
- [7] NetDiligence. "NetDiligence Publishes Sixteenth Annual Cyber Claims Study." *NetDiligence*, 15 Sept. 2026, <https://netdiligence.com/press-releases/netdiligence-releases-2026-cyber-claims-study/>. Accessed 30 Sept. 2026.
- [8] NetDiligence. "What 10,309 Cyber Claims Reveal about Cyber Risk in 2026." *NetDiligence*, 22 Sept. 2026, <https://netdiligence.com/blog/2026/09/2026-cyber-claims-study-key-findings/>. Accessed 30 Sept. 2026.
- [9] Swiss Re. "Swiss Re Sees Growing Protection Needs as Risks Become More Complex and Interconnected." *Swiss Re*, 7 Sept. 2026, <https://www.swissre.com/press-release/Swiss-Re-sees-growing-protection-needs-as-risks-become-more-complex-and-interconnected/14c62184-38e0-4c80-93c8-6ecf83fdda28>. Accessed 30 Sept. 2026.
- [10] Swiss Re Institute. "Insurance Demand across Lines and Lifecycle." *Time to Build: The Capex Super-Cycle*, Sigma 3/2026, Swiss Re, 2026, <https://www.swissre.com/institute/research/sigma-research/sigma-2026-03-time-to-build/03-2026-Insurance-demand-across-lines-and-lifecycle.html>. Accessed 30 Sept. 2026.

Webinars, Learning Hub & Research Reports

September webinar recordings, the DeNexus Learning Hub, and research reports on OT cyber risk quantification and management.

 Missed the September Webinars? Watch them here

 ON-DEMAND WEBINAR

DeRISK UWA — Underwriting OT Cyber Risk, End to End

SEP 23, 2026 · 45 MINS

Kevin Hamman (DeNexus), George Mawdsley (DeNexus), Jack Chamberlain (Chaucer)

Watch now →

 ON-DEMAND WEBINAR

Building a Multi-Year OT Cyber Risk Management Program

SEP 30, 2026 · 45 MINS

Kevin Hamman (DeNexus) & Scott Hooper (Clearway)

Watch now →

 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

● Available for download

 The US AI Data Center Industrial Complex

[Download PDF →](#)

 The Impact of the Iran War on Industrial Cyber Risk

[Download PDF →](#)

 Manufacturing Sector Cyber Incidents — H1 2026

[Download PDF →](#)

 A Framework for Infrastructure Lenders

[Download PDF →](#)

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 →