DENEXUS™

JULY 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

Thought Leadership

A practical OT risk playbook: Quantify, Reduce, Transfer

The operating model for cyber-physical risk management

Thought Leadership

A practical OT risk playbook: Quantify, Reduce, Transfer

The first half of this year did one thing well: it established a shared language. OT cyber-physical risk is its own class. Tail risk dominates the consequence picture. The insurance gap between cyber and property coverage is structural — not incidental, not temporary, not something better policy language will fix. That foundation matters. But understanding a problem is not the same as having a program.

What follows is the operating model.

Three moves: **Quantify, Reduce, Transfer**. Each depends on the one before it, and none works well in isolation. Quantification creates the shared currency — expected loss and tail loss at facility level, traceable to specific scenarios, grounded in assumptions that can be defended on first principles rather than benchmark averages. Reduction bends the loss curve by prioritizing improvements that change feasible outcomes under real constraints: outage windows, vendor dependencies, staffing models, safety requirements. Not what scores worst on a generic framework. Transfer moves residual risk to markets that can price it, with evidence structured to earn capacity rather than friction.

These three moves are not sequential project milestones. That is the mistake most programs make — treating them as phases, completing one before starting the next, and wondering why the results don't compound. The organizations that get ahead run them in parallel: always quantifying, always reducing, always maintaining transfer-ready evidence. That discipline is what credibility looks like to a board and to an underwriter. Same language. Same evidence. Different questions answered.

Quantify using consequence pathways and bounded assumptions. Decision-grade is not actuarial perfection. It is a number that can be explained, defended, and updated as evidence changes. If you cannot tell your CFO which assumptions move the answer materially, the number is not ready for a board conversation or a market conversation.

Reduce by prioritizing actions that change feasible outcomes under actual operational constraints. Constraint-aware sequencing is the discipline that converts plans into execution. Plans that stall because they were built for ideal conditions produce no risk reduction — and no evidence of risk reduction. Both are damaging: one to the program, one to the renewal.

Transfer becomes tractable when evidence is standardized and scenarios are credible. The market does not pay for narrative complexity. It pays for structured exposure that capital can compare and aggregate. Comparability is the precondition for capacity — not relationships, not narrative, not the quality of your broker's presentation. The evidence is the argument.

Three things worth doing this month. First: choose two or three credible scenarios per critical facility and identify the mitigations that move outcomes. Start where consequence is highest, not where the headlines are loudest. Second: track improvements as changes in drivers — feasibility, restoration time, access path constraints — not ticket counts. The right metric is what moved the loss curve. Third: build a market-ready narrative with bounded scenarios, proof bundles, and a clear what-changed summary. Both sides of the placement conversation need to be able to follow it.

Next month

why audit trails decide whether a quantification number is usable.

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

Industry News

Regulation, Threats & Insurance Developments

CISA directives, Check Point vulnerabilities, UK NCSC reports, and CrowdStrike insurance initiatives

Regulation & Policy Developments

CISA BOD 26-04: Prioritizing Security Updates Based on Risk

CISA issued Binding Operational Directive 26-04, "Prioritizing Security Updates Based on Risk," on June 10, requiring U.S. federal civilian agencies to prioritize remediation based on actual risk signals rather than CVSS severity alone. The directive uses factors such as asset exposure, CISA KEV status, exploit automation, and technical impact to determine remediation urgency, with CISA's implementation guidance tying the model to recurring exposure reporting and vulnerability-response workflows. For OT and industrial operators, the practical lesson is clear: patching programs need to understand what is exposed, exploitable, and operationally consequential, not just what is "critical" on paper. This is especially relevant in OT environments where maintenance windows, safety constraints, and change-control requirements make blanket patching unrealistic. [1] (CISA)

Threat Signals / Major Exploited Vulnerabilities

Check Point VPN zero-day exploitation shows why remote-access exposure remains a high-priority OT pathway.

Check Point disclosed active exploitation of CVE-2026-50751, a critical authentication-bypass vulnerability affecting Remote Access VPN and Mobile Access deployments using deprecated IKEv1; exploitation can allow an attacker to establish a VPN session without a valid user password [2]. CISA added the vulnerability to its Known Exploited Vulnerabilities catalog on June 8 [3], and Check Point said exploitation had been observed since May 7, was limited to a few dozen targeted organizations globally, and included one case of post-compromise activity associated with a Qilin ransomware affiliate [2]. This should be treated as a remote-access and perimeter-control risk, not a confirmed OT compromise story. For industrial organizations and insurers, the concern is that VPN and firewall compromise can provide a repeatable path into enterprise systems, vendor access zones, jump hosts, and OT-support environments, creating both business-interruption and aggregation risk [4]. (CheckPoint)

UK NCSC says hostile states are linked to most cyber incidents affecting critical systems.

The UK NCSC reported that it managed more than 200 cyber incidents affecting the UK's critical national infrastructure and supporting ecosystem in the year to May 2026, with around 75% believed to be linked to hostile state actors. NCSC CEO Dr. Richard Horne named Russia, China, and Iran as examples of states increasingly targeting the systems that underpin essential services. For OT leaders, this reinforces the need to plan beyond ransomware economics: some adversaries may seek espionage, pre-positioning, coercive leverage, disruption, or societal impact. For cyber insurers and risk-transfer stakeholders, the signal is equally important because state-linked activity complicates attribution, accumulation modeling, resilience assumptions, and policy wording around systemic or conflict-linked scenarios. [5] (National Cyber Security Centre)

Cyber Insurance & Risk Transfer

CrowdStrike brings insurers and brokers into Project QuiltWorks to address frontier-AI financial exposure.

CrowdStrike expanded Project QuiltWorks with Coalition, Liberty Mutual Insurance, Lockton, Resilience, and Marsh, positioning the initiative as a coordinated model for identifying, remediating, and financially mitigating frontier-AI cyber risk. CrowdStrike says QuiltWorks combines frontier models from OpenAI and Anthropic with AI-driven vulnerability discovery, adversary-informed prioritization, remediation services, and now insurance-sector input on financial modeling and mitigation.

For DeNexus readers, **the important point is not that this solves AI risk, but that cyber insurance, security telemetry, remediation, and financial exposure modeling are starting to converge around the same problem**: AI can accelerate vulnerability discovery and compress the time between exposure and exploitation. That creates a new underwriting question for industrial organizations: can risk owners show not only that vulnerabilities are found, but that financially material attack paths are prioritized and remediated before they become losses? [6] (CrowdStrike)

From DeNexus

Six national cyber agencies just put OT on the board agenda — José M. Seara on what industrial leaders should do with it.

On June 1, the heads of CISA, NSA, the UK NCSC, and their Canadian, Australian, and New Zealand counterparts published a rare joint statement on AI and cyber risk, warning that the timeline for AI-amplified attacks is months, not years, and calling unsupported systems "strategic liabilities". In his latest post, DeNexus Founder & CEO José M. Seara unpacks what the statement means specifically for industrial operators: why AI-accelerated vulnerability discovery adds work to already saturated OT remediation systems, why the perimeter is the real near-term exposure, and why the same AI capability compressing discovery-to-exploit for attackers can compress discovery-to-remediation for defenders. His conclusion: legacy OT exposure now needs to be quantified financially, sequenced by what actually moves the loss curve, and maintained as evidence on a governance cadence — not assembled at renewal. [7] (DeNexus blog)

→ **Read More**

Works Cited

[1] Cybersecurity and Infrastructure Security Agency. "BOD 26-04: Prioritizing Security Updates Based on Risk." *CISA*, 10 June 2026, https://www.cisa.gov/news-events/directives/bod-26-04-prioritizing-security-updates-based-risk.

[2] Finkelstein, Lotem. "Security Advisory – Action Required – Active Exploitation of Check Point VPN Authentication Bypass (CVE-2026-50751)." *Check Point Blog*, Check Point Software Technologies, 8 June 2026, https://blog.checkpoint.com/security/check-point-releases-important-hotfix-for-vulnerabilities-in-deprecated-ikev1-vpn-protocol/.

[3] Cybersecurity and Infrastructure Security Agency. "CISA Adds Two Known Exploited Vulnerabilities to Catalog." *CISA*, 8 June 2026, https://www.cisa.gov/news-events/alerts/2026/06/08/cisa-adds-two-known-exploited-vulnerabilities-catalog.

[4] Arghire, Ionut. "Check Point VPN Zero-Day Exploited in Qilin Ransomware Attacks." *SecurityWeek*, 9 June 2026, https://www.securityweek.com/check-point-vpn-zero-day-exploited-in-qilin-ransomware-attacks/.

[5] National Cyber Security Centre. "NCSC CEO: Hostile States Linked to Three-Quarters of Cyber Attacks Affecting UK's Critical Systems." *NCSC*, 17 June 2026, https://www.ncsc.gov.uk/news/ncsc-ceo-hostile-states-linked-to-three-quarters-of-cyber-attacks.

[6] CrowdStrike. "CrowdStrike Expands Project QuiltWorks with Cyber Insurance Industry Leaders to Combat Financial Exposure to Frontier AI Risk." *CrowdStrike Investor Relations*, 28 May 2026, https://ir.crowdstrike.com/news-releases/news-release-details/crowdstrike-expands-project-quiltworks-cyber-insurance-industry/.

[7] Seara, Jose M. "When Six Governments Say the Same Thing, It's Time to Listen — and Act." *DeNexus*, 29 June 2026, https://www.denexus.io/resources/when-six-governments-say-the-same-thing-its-time-to-listen-and-act

Denexus in July

Webinars, Learning Hub & Upcoming Events

Explore our on-demand webinars, new Learning Hub, upcoming white papers, and industry events featuring the DeNexus team.

Two Live Webinar Sessions Now Available On Demand

Quantified OT Cyber Risk: From Exposure to Reduction

Walks through how DeRISK CRQ and QVM translate OT exposure into financial terms — Expected Annual Loss, Value at Risk — and turn those numbers into a prioritized reduction program.

60 minutes Live demo + Q&A

→ Watch The Replay

Industrial OT Cyber Underwriting: From Submission to Binding Decision

Shows the insurance side: a live demo of DeRISK UWA Agentic and the three-tier approach that takes underwriters from raw submission to a bindable decision.

60 minutes Live demo + Q&A

→ Watch The Replay

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

Three White Papers on the Way

US Data Centers: Cyber Risk Profile

Examining the cyber risk profile of the infrastructure layer underneath the AI buildout — coming July 2026

Iran War / Industrial OT Risk
Coming August 2026

Edge Models / Industrial Cyber Risk
Coming September 2026

Upcoming Event

ISA/ISASecure
Jose Seara – Founder & CEO, DeNexus
9 Sep 2026 Virtual

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