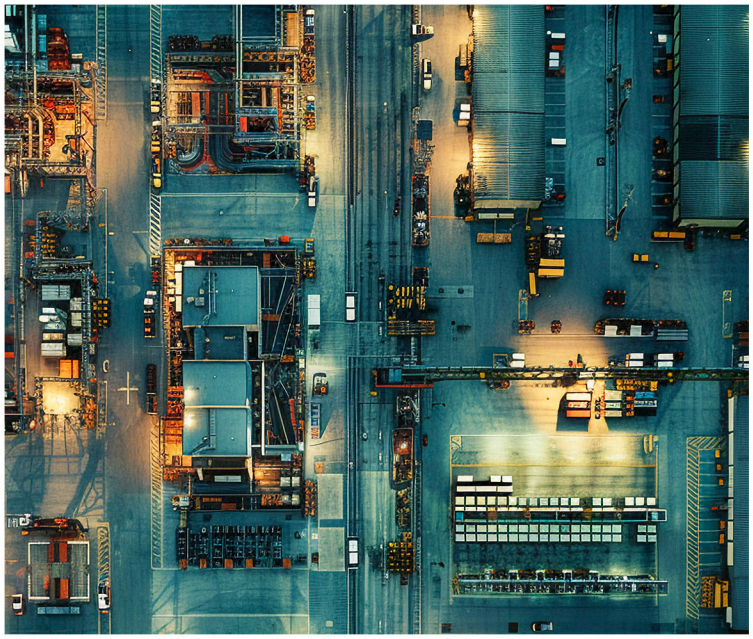
OT Cyber isn't IT Cyber: Why The Risk Behaves Differently

OT cyber-physical risk is fundamentally different from traditional IT cyber risk. The primary outcomes are operational: uptime, safety, quality, equipment integrity, and cascading impacts. That difference changes how leaders govern risk and how markets underwrite it.



WHAT MATTERS THIS MONTH

Breach is not the outcome. Loss is shaped by restoration economics, operational constraints, and dependencies.

Facilities are the exposure unit. Portfolios are distributions, and correlation often comes from shared architectures, vendors, and access patterns.

Evidence beats volume. Decision-grade and underwriting-grade conversations require a compact, defensible set of artifacts, not longer questionnaires.

What you can do now

- Industrial leaders: establish a minimum facility truth dataset and assign ownership for keeping it current.
- OT and security teams: make remote access pathways, segmentation reality, and restoration dependencies explicit and testable.
- Brokers, markets, and capital: push for standardized proof bundles and bounded assumptions that can be audited.

Next month

- Consequence pathways: how OT loss actually crystallizes after containment.
- Educational content only. Not legal, coverage, or underwriting advice.

Highlights - OT Cybersecurity Industry News

- **Attacks and incidents:** Polish Energy Infrastructure, Romania, ...
- **Regulation and policy:** updated TSA pipeline directive, proposal to revise EU cyber act, ...
- **Guidance:** Secure OT Connectivity Principles
- **Activity trends:** Forescout reports 71% of exploited vulnerabilities in 2025, were NOT on CISA KEV list.
- **Vulnerabilities:** CISA adds Watchguard, Fortinet, VMware vCenter to KEV list.
- **Cyber Insurance and risk transfer:** Cyber insurance stable but softening,

Attacks and Incidents (Reported in January 2026)

- **Poland — Energy infrastructure / Distributed Energy Resources (DER):** Government said attacks on 29–30 Dec 2025 targeted two CHP plants and a renewables management/dispatch system; Dragos described coordinated targeting of DER sites and OT impacts including loss of view/control and denial-of-service conditions, with no reported outage. [3], [1], [2], [4].
- **Romania — Water sector:** DNSC reported ransomware affecting Romanian Waters IT systems (including ~1,000 IT&C systems across 10 basin administrations), while stating OT/hydrotechnical operations were not affected; January coverage emphasized the critical services context. [19], [20].
- **Romania — Energy producer:** Holiday-period ransomware impacted Oltenia Energy Complex business IT infrastructure (per company statement cited in January reporting). [20].
- **Venezuela — Oil & gas:** Reuters reported PDVSA's administrative systems had not fully recovered from a December cyberattack, forcing isolation of terminals/oilfields/refineries from central systems and use of manual records to sustain operations. [21].

Regulation and Policy Developments (OT-Relevant)

- **EU — Proposal for revised Cybersecurity Act:** The Commission proposed a revised Cybersecurity Act and targeted NIS2 amendments aimed at clarifying jurisdiction and easing compliance while reinforcing ENISA's coordinating role. [14], [15], [16]. An EU Parliament think-tank briefing summarized expected focus areas for Cybersecurity Act review work. [35].
- **UK — Cyber Security and Resilience (NIS) Bill:** The Bill received its Second Reading on 6 Jan 2026 and progressed for scrutiny; it is positioned as an update/extension to the UK's NIS regulatory framework for essential services and digital providers. [17], [18].
- **US — Transportation security directives:** TSA's cybersecurity Security Directives for rail/public transportation and pipeline operators show January 2026 updates (including SD 1580-21-01E and updated pipeline directive). [12], [13], [36].
- **US — Transit sector guidance:** NIST released an initial public draft of NIST IR 8576 (Transit CSF Community Profile) as a voluntary, risk-based guide for transit agencies managing IT/OT risk. [10], [11].

Threats, Guidance, and Vulnerability Signal (OT Relevant)

- **OT connectivity:** CISA and partner agencies published Secure Connectivity Principles for OT (eight principles) intended as target end-states for designing and governing OT connectivity. [7], [8], [9].
- **ICS vulnerability disclosures:** CISA issued multiple ICS Advisories in January (e.g., Schneider Electric, Rockwell Automation, Weintek, Johnson Controls, iba Systems, AVEVA); partner summaries (e.g., Canada) highlighted the volume of advisories published in late January. [24], [25], [26], [37].
- **Known Exploited Vulnerabilities (KEV):** January KEV additions included OT-relevant "edge and management" technologies—Fortinet FortiOS/Fortizer (FortiCloud SSO auth bypass, CVE-2026-24858) and Broadcom VMware vCenter Server (DCERPC heap overflow/RCE risk, CVE-2024-37079)—reinforcing priority patching and validation of OT remote-access, segmentation, and management-plane controls. (and continued attention to WatchGuard Firebox CVE-2025-14733, a late-December KEV addition). [38], [39], [40], [41].
- Forescout threat roundup reports 71% of exploited vulnerabilities in 2025 were NOT in the CISA KEV catalog [42].
- **Activity trends:** A Cyble/CRIL report published in January described increased hacktivist and cybercriminal activity affecting ICS/OT environments and highlighted continued exploitation of industrial vulnerabilities. Forescout report shows 48% YoY increase in Web App attacks (aka., T1190 Exploit Public-Facing Application) and 84% surge in OT protocol attacks (Modbus, EIP, BACnet, etc.). [27], [42].

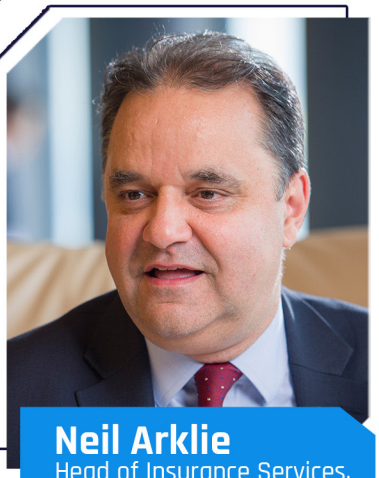
OT Cyber Insurance and Risk Transfer (Market Signals in January)

- **Pricing/market tone:** Gallagher and industry coverage described a broadly competitive market with stable-to-softening pricing, while underwriting focus persists on ransomware, third-party/supply-chain risk and business interruption. [28], [29].
- **Systemic-risk framing:** January reinsurance/market commentary highlighted abundant capacity at 1.1 renewals and growing attention to correlated/systemic cyber loss scenarios, relevant to OT operators with shared dependencies and outage exposure. [30], [31].
- **Risk perception:** Allianz's 2026 Risk Barometer ranked cyber incidents as a top business risk; WEF's Global Cybersecurity Outlook 2026 emphasized increasing cyber risk amid geopolitical and technology shifts. [32], [33].

S4x26: ICS Security Conference

February, 23rd – 26th, 2026

Speaker



Neil Arklie
Head of Insurance Services,
DeNexus

Topic

Closing the Cyber-Physical Risk Capital Gap in Insurance

Tuesday,
24th February, 2026

Afternoon Session,
2:00 - 2:30pm

Attending

Jose M. Seara
CEO & Founder,
DeNexus

Kevin Hamman
Product Delivery Manager,
DeNexus

Donovan Tindill
Director of OT Cybersecurity,
DeNexus

Andrew Gurciullo
Account Executive
DeNexus

Looking forward to connecting with you

www.denexus.io info@denexus.io

References

[1] Dragos – Poland Power Grid Attack Targets Distributed Energy Facilities (Jan 28, 2026)

[2] Dragos – ELECTRUM: Targeting Poland's Electric Sector (report landing page)

[3] Chancellery of the Prime Minister (Gov.pl) – Poland Stops Cyberattacks on Energy Infrastructure (Jan 15, 2026)

[4] Reuters – Massive cyberattack on Polish power system in December failed, minister says (Jan 13, 2026)

[5] Reuters – Russian military intelligence hackers likely behind December cyberattacks in Poland, researchers say (Jan 23, 2026)

[6] ESET Research – Sandworm behind cyberattack on Poland's power grid in late 2025 (DynoWiper) (Jan 23, 2026)

[7] CISA – News: CISA, UK NCSC, FBI unveil principles to combat cyber risks to OT (Jan 14, 2026)

[8] UK NCSC – Secure connectivity principles for operational technology (Published Jan 14, 2026)

[9] CISA – Secure Connectivity Principles for Operational Technology (Publish date Jan 14, 2026)

[10] NIST CSRC – News: Draft Transit Cybersecurity Framework (CSF) Community Profile (Jan 22, 2026)

[11] NIST – NIST IR 8576 ipd: Transit Cybersecurity Framework Community Profile (Jan 2026) (PDF)

[12] TSA – Security Directives and Emergency Amendments page (January 2026 updates)

[13] TSA – Security Directive 1580-21-01E (Rail cybersecurity) (effective Jan 16, 2026) (PDF)

[14] European Commission – Cybersecurity Package Q&A (Jan 20, 2026)

[15] European Commission – Press release: Commission strengthens EU cybersecurity resilience and capabilities (IP_26_105) (Jan 19, 2026)

[16] European Commission – Proposal: targeted NIS2 amendments / simplification measures (Jan 20, 2026)

[17] UK Parliament – Call for evidence / progress on Cyber Security and Resilience (NIS) Bill (Jan 7, 2026)

[18] UK Parliament – Cyber Security and Resilience (Network and Information Systems) Bill (bill page)

[19] Romanian National Cyber Security Directorate (DNSC) – Press release on ransomware attack against Romanian Waters (Dec 2025)

[20] Industrial Cyber – Romanian water authority, energy producer hit by cyber attacks (Jan 5, 2026)

[21] Reuters – Venezuela's PDVSA administrative system not fully recovered from cyberattack (Jan 3, 2026)

[22] INCIBE (Spain) – Endesa notifies customers of personal-data leak (Jan 2026)

[23] SecurityWeek – Spanish Energy Company Endesa Hacked (Jan 13, 2026)

[24] CISA (GovDelivery) – CISA Releases 10 Industrial Control Systems Advisories (Jan 22, 2026)

[25] CISA – ICS Advisory ICSA-26-027-01: iba Systems ibaPDA (Jan 27, 2026)

[26] Canadian Centre for Cyber Security – [Control systems] CISA ICS security advisories (AV26-051) (Jan 26, 2026)

[27] Infosecurity Magazine – Cyber Threat Actors Ramp Up Attacks on Industrial Environments (Jan 15, 2026)

[28] CFO Dive – Cyber insurance prices set to hold steady through mid-2026 (Jan 27, 2026)

[29] Gallagher (AJG) – 2026 Cyber Insurance Market Outlook (Jan 17, 2026)

[30] Aon – Reinsurance Market Dynamics: January 2026 Renewals (PDF)

[31] Reinsurance News – Cyber market benefited from more-than-adequate capacity at 1.1 (Jan 5, 2026)

[32] Allianz Commercial – Allianz Risk Barometer 2026 (PDF)

[33] World Economic Forum – Global Cybersecurity Outlook 2026 (PDF) (Jan 17, 2026)

[34] CISA – Alert: CISA Adds Five Known Exploited Vulnerabilities to Catalog (Jan 26, 2026)

[35] European Parliament Think Tank – Cybersecurity Act review: What to expect (Jan 5, 2026)

[36] TSA – Pipeline Security Directive (signed SD Pipeline 2021-01G) (Jan 2026) (PDF)

[37] CISA – ICS Advisory ICSA-26-015-01: AVEVA Process Optimization (Jan 15, 2026)

[38] CISA (cisagov/kev-data) – Known Exploited Vulnerabilities (KEV) Catalog data feed (CSV) (Jan 2026)

[39] Fortinet FortiGuard PSIRT – FG-IR-26-060: Administrative FortiCloud SSO authentication bypass (CVE-2026-24858) (Jan 27, 2026)

[40] Advisory VMSA-2024-0012.1: VMware vCenter Server updates (includes CVE-2024-37079) (Updated Jan 23, 2026)**

[41] WatchGuard PSIRT – WGSA-2025-00027: Fireware OS iked out-of-bounds write (CVE-2025-14733) (Dec 18, 2025)

[42] Forescout Research 2025 Threat Roundup