DENEXUS™

OT Tail Risk: Cascades, Feasibility, and Bounded Uncertainty

THOUGHT LEADERSHIP

OT cyber-physical risk behaves like a fat-tail problem: severe outcomes dominate the economics. This is why checklists and generic scoring often mislead. Tail outcomes are driven by cascades, dependencies, and feasibility.

WHAT MATTERS THIS MONTH

Cascades create tail loss.
Interdependencies and common-mode failures amplify severity.

Scenario credibility is central.
Feasibility, prerequisites, and stopping points must be explicit and defensible.

Bounded uncertainty is decision-usable.
Assumptions should be versioned, traceable, and sensitivity-tested.

WHAT YOU CAN DO NOW

Stress test plausible scenarios.
Stress test a small set of plausible scenarios per critical facility.

Introduce a scenario credibility
Introduce a simple scenario credibility scorecard (feasibility, prerequisites, stopping points, restoration drivers).

Prioritize auditability for markets.
For markets, prioritize auditability over sophistication: traceable inputs and bounded assumptions.

COMING NEXT MONTH

The OT cyber insurance gap: where recoverability is decided early.

DENEXUS™

OT CYBER INCIDENTS RESULTING IN PROPERTY DAMAGE

A FIELD GUIDE TO PUBLICLY REPORTED CYBER-PHYSICAL LOSS EVENTS

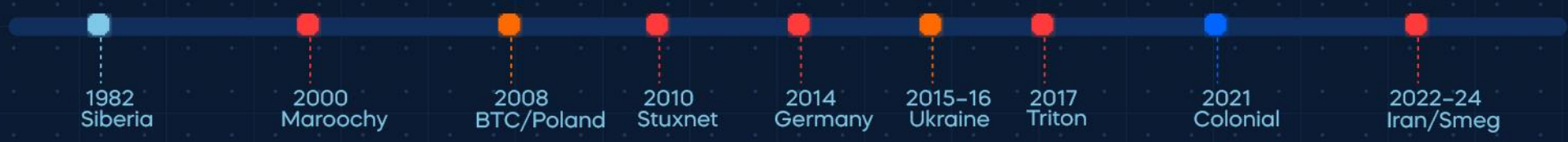
8 Incidents
MALICIOUS: MANIPULATION
Malicious OT cyber incidents with property damage
1982 – 2022

MALICIOUS: FIRMWARE
Firmware corruption / disk encryption (wipers)
2015 – 2023

ACCIDENTAL OT
Non-malicious failures with physical consequences

OTHER AFFECTING OT
IT-OT uncertainty driving operational shutdown
2021 – 2024

INCIDENT TIMELINE — 40 YEAR SEARCH: MALICIOUS OT CYBER INCIDENTS WITH PROPERTY DAMAGE



3 KEY PATTERNS ACROSS ALL INCIDENTS

PHYSICS DRIVES LOSS

Cyber-physical loss is driven by physics, not by attacker intent. Once pressure, temp, or alarm limits are violated, the process "does what it does."

IT → OT PIVOT

Many pathways begin with IT compromise (phishing, credential theft) and become catastrophic only after lateral movement into OT networks.

NEAR MISSES MATTER

Events like Triton show that absence of explosion ≠ low risk. Near misses inform credible loss scenarios and reveal attacker capabilities.

LANDMARK CASE STUDIES

2009–2010	2014	2015–2016	2017	2021	2022
STUXNET	STEEL MILL	UKRAINE GRID	TRITON	COLONIAL	IRAN STEEL
Iran · Nuclear	Germany · Metals	Ukraine · Electric T&D	Saudi Arabia · Petrochem	USA · Oil & Gas	Iran · Metals
PLC logic altered, centrifuges destroyed	Blast furnace meltdown, physical damage	225,000 customers lost power, firmware wiped	Safety system targeted, near-miss explosion	IT ransomware, pipeline shut down, $5M paid	Molten steel overflow, factory fire
Nation-State Targeted	Crime Syndicate Targeted	Nation-State Targeted	Nation-State Targeted	Crime Syndicate Indirect	Hacktivist Targeted

WHAT THIS MEANS FOR LEADERSHIP

OT cyber risk must be managed as cyber-physical risk. Move beyond qualitative heat maps — financially quantify expected loss to enable: (1) Prioritize controls by measurable risk reduction (2) Connect OT security to business outcomes (3) Support underwriting and risk transfer with defensible cyber-physical loss estimates.

CLICK HERE TO READ FULL REPORT

DENEXUS™

POLAND ENERGY SECTOR CYBER INCIDENT

ATTACK SCOPE

30+
Wind and Solar Farms
Loss of visibility and remote control
Renewable Energy Sites

2
CHP Generation Plants
Sabotage via wiper malware
Blocked by endpoint controls

1
Manufacturing Company
Opportunistic wiper attempt
Same Dynowiper Family

DEFENSE OUTCOME
No blackout. No national grid destabilization.
Rapid detection limited impact.

INCIDENT TIMELINE

- **29 DEC 2025** — Initial Attack and Disruption
- **15 JAN 2026** — KPRM Official Briefing
- **28 JAN 2026** — Dragos Intel Brief Published
- **30 JAN 2026** — CERT Polska and ESET Reports
- **6 FEB 2026** — Elastic Labs Analysis
- **10 FEB 2026** — U.S. CISA Alert Issued

ATTACK MECHANICS AND TECHNICAL FINDINGS

INITIAL ACCESS
No MFA enforced
Internet-facing devices

→

LATERAL MOVEMENT
IT to OT pivot
Credential abuse
Long dwell at CHP
Sensitive data exfiltrated

→

OT DEVICE DAMAGE
Firmware corruption
System file deletion
RTU and HMI damage
Loss of view and control

→

DYNOWIPER MALWARE
16-byte random file overwrite
Targets fixed and removable drives
Forces reboot to complete destruction
Blocked by canary-file monitoring

ATTRIBUTION (DIVERGENT ACROSS SOURCES)

CERT POLSKA
Infrastructure overlap:
Static Tundra / Berserk Bear
Ghost Blizzard / Dragonfly
First destructive use by cluster

DRAGOS
ELECTRUM threat group
Moderate confidence
TTP overlaps with Sandworm
First major DER attack at scale

ESET RESEARCH
DynoWiper to Sandworm
Medium confidence
Russia-aligned APT
Prior wiper TTP overlap

KPRM / POLAND GOVT
Russian intelligence services
Legislative response launched
National Cybersecurity Act
strengthened OT and IT rules

CRITICAL VULNERABILITIES EXPLOITED

01 DER Operational Dependency on Communications
Loss of supervisory control creates safety, reliability and compliance consequences

02 Credential Risk at Fleet Scale
Password reuse across 30+ sites; default credentials; one-to-many blast radius

03 OT and ICS Device Hardening Gaps
Default accounts on RTUs, relays, serial servers; no configuration governance

04 Insufficient IT to OT Segmentation
Flat networks allowed lateral movement from perimeter directly to operational assets

05 Edge Device Tampering and Evidence Loss
Factory-resets of perimeter devices destroyed forensic telemetry and logging

06 Limited OT-Native Monitoring
No protocol-aware detection; insufficient log retention for post-incident investigation

07 Enterprise Identity to Wiper Distribution
Domain privilege abuse enabled rapid wiper payload deployment at scale

CLICK HERE TO READ FULL REPORT

DENEXUS™

MEET US AT

Industry Events

Spring & Summer 2026 · Speaking, Exhibiting & Attending

6 EVENTS | APR – JUN 2026

WHERE TO FIND US

Donovan Tindill
Director of OT Cybersecurity

LEVEL ZER0 OT CYBER SECURITY CONFERENCE

Applying Financial Quantification of Risk in ICS/OT Cybersecurity Decision-Making

VENUE
Atlanta, GA

DATE
April 20 – April 22, 2026

April 22

Cyber Insurance Awards

Chicago, Illinois · Jose Seara

April 27

ASTIN Cyber Workshop

London, United Kingdom · Jose Seara

May 7

Fortinet

Detroit, Michigan · Jose Seara

June 1-3

Gartner Risk Summit

National Harbor, MD · Jose Seara

Jun 8-10

SANS ICS Security Summit

Orlando, Florida · Donovan, Tindill

Jun 8-10

Fortinet OT Summit

Virtual · Donovan Tindill

Let's connect at these events
Schedule a one-on-one meeting · contact@denexus.io

BOOK A MEETING

OT CYBERSECURITY, OT CYBER RISK, AND CYBER INSURANCE

OT CYBER ATTACKS AND INCIDENTS

STRYKER — MEDICAL DEVICES.

Stryker's March 11 cyberattack disrupted order processing, manufacturing, and shipping across its Microsoft & Intune environment, and the company warned the operational hit could still affect revenue, operating income, cash flow, and liquidity. The public record suggests patient-care disruption risk—not a confirmed product-safety compromise: Stryker says connected and life-saving technologies remained safe to use and it did not believe patient-related services were disrupted, but Reuters reported that some patient-specific surgeries were delayed because personalized inventory could not be delivered on time. [1] [2] [3]

NOVA SCOTIA POWER — ELECTRIC UTILITY.

Nova Scotia Power says a sophisticated foreign threat actor stole customer and internal data, destroyed or locked down key business systems, and triggered a long-tail recovery that stretched well beyond the initial incident. Power generation and delivery were not affected, and the company says meters kept measuring usage accurately; however, the cyberattack prevented meter data from flowing back into utility systems, forcing estimated bills and leaving meter-to-billing reconnection work running into the end of March. Public statements point to disruption in the meter-data path or billing integration—not public evidence that the physical meters themselves were manipulated. [6] [7]

UMMC — HEALTHCARE.

UMMC restored normal clinic operations on March 2 after a nine-day cyber crisis, but the financial damage outlasted the outage. The medical center said patient care was disproportionately affected, and Mississippi Today reported roughly 650 delayed surgeries plus a February operating-revenue shortfall of about $34.2 million—around 20% below budget—showing how long business interruption can linger even after systems come back. [4] [5]

REGULATION AND POLICY DEVELOPMENTS

UK CYBER SECURITY AND RESILIENCE BILL.

The UK Cyber Security and Resilience (Network and Information Systems) Bill cleared committee and now sits at the report-stage gate in the Commons, with a committee-amended version published on February 25 and the next debate date still to be set. It is not yet law: the bill must still clear report stage and third reading in the Commons, pass the Lords, and receive Royal Assent; even then, implementation will be phased, with some provisions starting soon after enactment and others depending on later commencement and secondary legislation. If enacted, it would expand the NIS regime to data centres, managed service providers, and large load controllers. [8] [9]

U.S. FCC COVERED LIST — FOREIGN-MADE CONSUMER ROUTERS. The FCC has expanded its Covered List to include consumer-grade routers produced in foreign countries, which means new models in that category can no longer receive FCC authorization unless conditionally approved; previously authorized models are not automatically barred from sale or use. For OT-adjacent environments, this matters because low-cost routers of the sort used in field offices, contractor trailers, temporary sites, or remote maintenance setups can become weak links; examples of products in the affected class include TP-Link's Archer AX1800 and AX3000 home and small-business routers. [10] [11] [12] [13]

FERC APPROVES CIP-003-11 FOR LOW-IMPACT BES CYBER SYSTEMS. FERC has approved CIP-003-11, raising the baseline for utilities that operate low-impact BES Cyber Systems by requiring stronger controls for remote-user authentication, protection of authentication information in transit, and detection of malicious communications to and from externally reachable low-impact assets. The final rule takes effect on May 26, 2026, while the NERC implementation plan gives registered entities a 36-month runway before compliance obligations begin. [14] [15] [16]

OT CYBERSECURITY, OT CYBER RISK, AND CYBER INSURANCE

THREAT SIGNALS

• **ODNI 2026 Annual Threat Assessment.** ODNI's 2026 Annual Threat Assessment says China remains the most active and persistent cyber threat to U.S. government, private-sector, and critical-infrastructure networks, while Russia, Iran, North Korea, and ransomware actors continue to pose serious operational risk. For OT security leaders and cyber insurers, the actionable message is to treat nation-state pre-positioning, disruptive critical-infrastructure risk, and ransomware accumulation as part of the same loss conversation—not separate silos. [17]

• **Google Mandiant M-Trends 2026.** Mandiant reports that exploits accounted for 32% of initial intrusions and voice phishing for 11%, with median dwell time at 14 days; it also warns that ransomware actors are increasingly targeting backup systems, identity services, and virtualization management layers to deny recovery. For OT defenders, that elevates edge devices and recovery infrastructure from 'IT support' issues to mission-critical controls; for insurers, it underscores why log retention, segmentation, and restore testing increasingly shape loss severity. [18]

• **Claroty Team82.** Claroty's review of 200-plus cyber-physical-system attacks found that 82% involved VNC or other insecure remote access, 66% involved HMI or SCADA compromise, and more than 45% hit manufacturing, water/wastewater, or power-generation targets. The practical takeaway is blunt: exposed remote-access paths and operator-facing systems remain some of the fastest routes to real-world operational impact, even for comparatively low-complexity threat actors. [19] [20]

CYBER INSURANCE AND RISK TRANSFER

CFC characterizes the U.S. cyber market as still competitive, but with claims activity rising enough to erode profitability and push some insurers toward rate increases on renewal books. The underwriting signal is that soft pricing no longer means soft risk: ransomware, data-only extortion, and AI-enabled attack acceleration are all pressuring carriers to differentiate more aggressively on controls and exposure quality. [31]

Coalition's 2026 claims data show initial ransomware demands up 47% to more than $1 million on average, even as 86% of victims refused to pay; 70% of ransomware incidents involved both encryption and data theft, which often doubled incident cost. At the same time, 64% of closed claims produced no out-of-pocket loss for policyholders, reinforcing the value of active incident response and rapid fund recovery rather than treating insurance as a passive reimbursement product. [33]

WTW's March guidance frames geopolitical cyber disruption as a balance-sheet problem, not just a security problem: operators need to quantify how an attack would affect earnings, liquidity, recovery timelines, and dependency risk across power, water, transport, telecom, and key suppliers. That is especially relevant to OT and industrial buyers because it turns the insurance question from 'Do we buy more?' into 'What should we retain, what should we transfer, and what could a prolonged outage really cost?' [32]

Aon says buyers still have a favorable placement window, but volatility is building underneath: the average global ransomware claim cost rose to $713,000 in 2025, up from $374,400 in 2024, while underwriting attention is increasingly focused on control maturity, vendor dependencies, AI, privacy, and systemic event exposure. The opportunity for industrial and infrastructure buyers is to use today's competition to improve structure and limits before market conditions harden further. [34] [35]

CISCO CATALYST SD-WAN EXPLOIT CHAIN (CVE-2026-20127 + CVE-2022-20775).

Government guidance says active exploitation has already enabled persistence and long-term access. OT relevance is real because Cisco positions SD-WAN for utilities and industrial environments—including substations, distribution automation, AMI or smart metering, and factory connectivity—and Censys identified roughly 600 internet-facing SD-WAN Manager instances, with nearly a quarter also exposing ports 22 and/or 830 associated with the exploit path. For cyber insurers, it is a reminder to watch for portfolio co-exposure: the same control-plane product can sit across many distributed-site insureds, so initial compromise activity today may surface later as business interruption, extortion, or OT loss claims. [21] [22] [23] [24] [25] [26] [27] [28] [29]

REFERENCES

[1] Stryker. “Customer Updates: Stryker Network Disruption.” Stryker, 11 Mar. 2026, https://www.stryker.com/us/en/about/news/2026/a-message-to-our-customers-03-2026.html

[2] Stryker Corporation. “8-K.” U.S. Securities and Exchange Commission, 12 Mar. 2026, https://www.sec.gov/Archives/edgar/data/310764/000119312526104431/d101097d8k.htm

[3] Reuters. “Stryker cyberattack delays surgeries for some patients, Bloomberg News reports.” Reuters, 18 Mar. 2026, https://www.reuters.com/business/healthcare-pharmaceuticals/stryker-cyberattack-delays-surgeries-some-patients-bloomberg-news-reports-2026-03-18/

[4] University of Mississippi Medical Center. “UMMC prioritizes care, learning during cyberattack.” UMMC, 2 Mar. 2026, https://umc.edu/news/News_Articles/2026/03/Cyberattack.html

[5] Gwen Dilworth. “UMMC revenue tumbled after February cyberattack.” Mississippi Today, 21 Mar. 2026, https://mississippitoday.org/2026/03/21/ummc-revenue-tumbled-cyberattack/

[6] Nova Scotia Power. “Our Commitments: Office of the Privacy Commissioner of Canada investigation.” Nova Scotia Power, 25 Mar. 2026, https://nspower.ca/about-us/articles/details/articles/2026/03/25/our-commitments--office-of-the-privacy-commissioner-of-canada-investigation

[7] Nova Scotia Power. “Cyber Incident Updates.” Nova Scotia Power, 27 Mar. 2026, https://nspower.ca/home---cyber

[8] UK Parliament. “Cyber Security and Resilience (Network and Information Systems) Bill.” UK Parliament, 26 Mar. 2026, https://bills.parliament.uk/bills/4035

[9] UK Government. “Summary of the Bill.” GOV.UK, 12 Nov. 2025, https://www.gov.uk/government/publications/cyber-security-and-resilience-network-and-information-systems-bill-factsheets/summary-of-the-bill

[10] Federal Communications Commission. “FCC Updates Covered List to Include Foreign-Made Consumer Routers, Prohibiting Approval of New Models.” Federal Communications Commission, 23 Mar. 2026, https://docs.fcc.gov/public/attachments/DOC-420034A1.pdf

[11] Federal Communications Commission. “DA 26-278: FCC’s Public Notice and Guidance on Routers Produced by Foreign Countries.” Federal Communications Commission, 20 Mar. 2026, https://docs.fcc.gov/public/attachments/DA-26-278A1.pdf

[12] TP-Link. “Archer AX1800.” TP-Link, https://www.tp-link.com/us/home-networking/wifi-router/archer-ax1800/

[13] TP-Link. “Archer AX3000.” TP-Link, https://www.tp-link.com/us/home-networking/wifi-router/archer-ax3000/

[14] Federal Energy Regulatory Commission. “FERC Action: New Reliability Safeguards for American Power Grid.” Federal Energy Regulatory Commission, 20 Mar. 2026, https://www.ferc.gov/news-events/news/ferc-action-new-reliability-safeguards-american-power-grid

[15] Federal Energy Regulatory Commission. “Order No. 918; Critical Infrastructure Protection Reliability Standard CIP-003-11—Cyber Security—Security Management Controls.” Federal Register, 24 Mar. 2026, https://www.federalregister.gov/documents/2026/03/24/2026-05711/order-no-918-critical-infrastructure-protection-reliability-standard-cip-003-11-cyber

[16] North American Electric Reliability Corporation. “CIP-003-11 Implementation Plan.” NERC, 12 June 2024, https://www.nerc.com/globalassets/standards/projects/2023-04/cip-003-11-implementation-plan_061224.pdf

[17] Office of the Director of National Intelligence. “2026 Annual Threat Assessment of the U.S. Intelligence Community.” ODNI, 18 Mar. 2026, https://www.dni.gov/files/ODNI/documents/assessments/ATA-2026-Unclassified-Report.pdf

DENEXUS™

REFERENCES

[18] Google Cloud / Mandiant. “M-Trends 2026: Data, Insights, and Strategies From the Frontlines.” Google Cloud Blog, 23 Mar. 2026, https://cloud.google.com/blog/topics/threat-intelligence/m-trends-2026

[19] Claroty Team82. “Analyzing CPS Attack Trends.” Claroty, 18 Mar. 2026, https://claroty.com/resources/reports/analyzing-cps-attack-trends

[20] Claroty. “New Research Finds Cybercriminals are Increasingly Targeting Global Critical Infrastructure via Direct Access to Cyber-Physical Systems.” Claroty, 18 Mar. 2026, https://claroty.com/press-releases/new-research-finds-cybercriminals-are-increasingly-targeting-global-critical-infrastructure-via-direct-access-to-cyber-physical-systems

[21] Cybersecurity and Infrastructure Security Agency. “ED 26-03: Mitigate Vulnerabilities in Cisco SD-WAN Systems.” CISA, 25 Feb. 2026, https://www.cisa.gov/news-events/directives/ed-26-03-mitigate-vulnerabilities-cisco-sd-wan-systems

[22] Cybersecurity and Infrastructure Security Agency. “Supplemental Direction to ED 26-03: Hunt and Hardening Guidance for Cisco SD-WAN Systems.” CISA, 25 Feb. 2026, https://www.cisa.gov/news-events/directives/supplemental-direction-ed-26-03-hunt-and-hardening-guidance-cisco-sd-wan-systems

[23] National Vulnerability Database. “CVE-2026-20127 Detail.” NVD, 26 Feb. 2026, https://nvd.nist.gov/vuln/detail/CVE-2026-20127

[24] National Vulnerability Database. “CVE-2022-20775 Detail.” NVD, https://nvd.nist.gov/vuln/detail/CVE-2022-20775

[25] Canadian Centre for Cyber Security. “Critical vulnerability affecting Cisco Catalyst SD-WAN (CVE-2026-20127).” Canadian Centre for Cyber Security, 25 Feb. 2026, https://www.cyber.gc.ca/en/alerts-advisories/al26-004-critical-vulnerability-affecting-cisco-catalyst-sd-wan-cve-2026-20127

[26] Censys. “February 27 Advisory: Cisco Catalyst SD-WAN Controller and Manager CVE-2026-20127.” Censys, 25 Feb. 2026, https://censys.com/advisory/cve-2026-20127/

[27] Cisco. “SD-WAN for Industrial Solutions Solution Brief.” Cisco, 11 May 2023, https://www.cisco.com/c/en/us/solutions/collateral/enterprise-networks/sd-wan/sd-wan-for-industrial-solution.html

[28] Cisco. “Power Utilities and Renewable Energy Design Zone.” Cisco, https://www.cisco.com/c/en/us/solutions/design-zone/industries/power-utilities.html

[29] Cisco. “Nestlé and Cisco SD-WAN Case Study.” Cisco, 1 Oct. 2025, https://www.cisco.com/site/us/en/about/case-studies-customer-stories/nestle.html

[30] Munich Re. “Cyber Insurance: Risks and Trends 2026.” Munich Re, 25 Mar. 2026, https://www.munichre.com/en/insights/cyber/cyber-insurance-risks-and-trends-2026.html

[31] CFC. “The US cyber market in 2026: Your questions answered.” CFC, 20 Mar. 2026, https://www.cfc.com/en-us/knowledge/resources/articles/2026/03/the-us-cyber-market-in-2026-your-questions-answered/

[32] Anthony Wilson and Omar Al-Shahery. “Risk leaders: How to strengthen cyber resilience against geopolitical disruption.” WTW, 16 Mar. 2026, https://www.wtwco.com/en-gb/insights/2026/03/risk-leaders-how-to-strengthen-cyber-resilience-against-geopolitical-disruption

[33] Coalition. “2026 Cyber Claims Report.” Coalition, 24 Mar. 2026, https://www.coalitioninc.com/en-ca/claims-report/2026

[34] Aon. “Cyber 2026: Evolving Threats Demand Strategic Leadership.” Aon, 27 Jan. 2026, https://www.aon.com/en/insights/articles/cyber-2026-evolving-threats-demand-strategic-leadership

[35] Aon. “Cyber and E&O: Market Remains Soft but Volatility Grows.” Aon, 19 Mar. 2026, https://www.aon.com/en/insights/articles/cyber-and-tech-e-and-o-market-report