DENEXUS™

# From Incident To Consequence

## The evidence chain that drives loss

March 2026 Newsletter

# From Incident To Consequence: The Evidence Chain That Drives Loss

In OT, the most important decisions happen after the initial event: detection, containment, recovery sequencing, restart constraints, and third-party dependencies. Loss is often determined by what is operationally feasible, not what the response procedure says.

## What matters this month

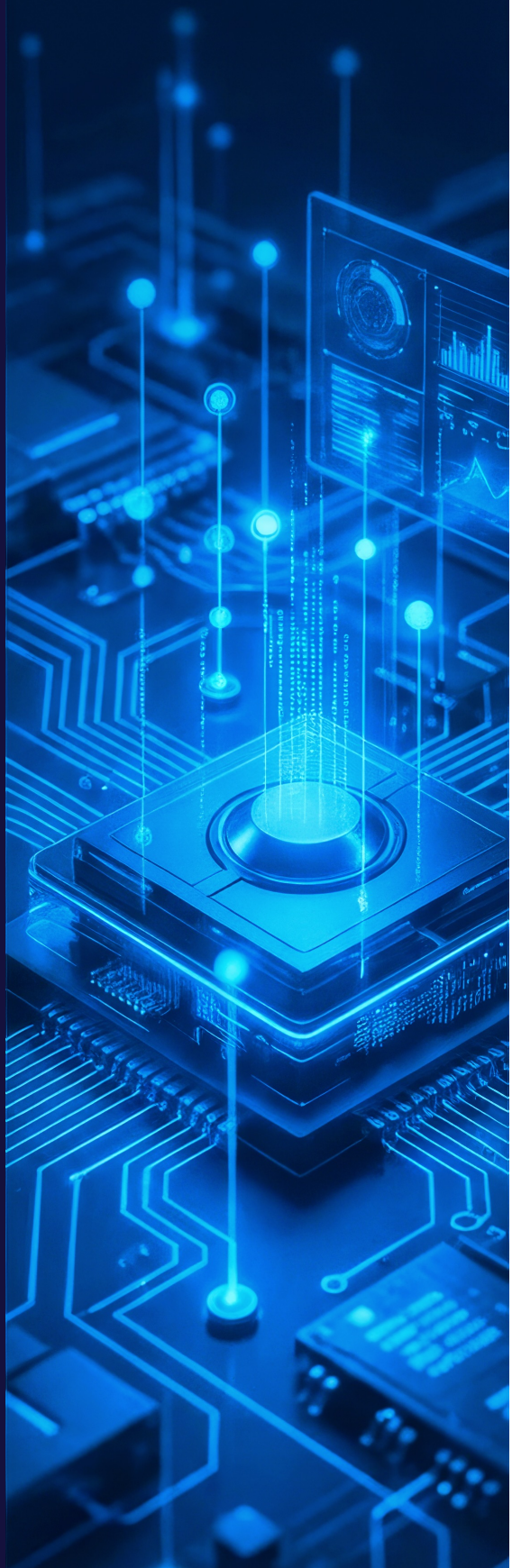
Complex consequence dependencies outweigh vulnerability counts. Many issues never become loss; some conditions cascade quickly.

Claims narratives live or die on the evidence chain. Cause, duration, restoration, and decision traceability matter.

Insurance loss accumulation begins with common structure. Shared vendors, shared tooling, and repeatable architectures create correlation.

## What you can do now

- Map key dependencies for critical facilities (remote access, virtualization, authentication, applications, vendors).
- Validate ICS/OT graceful degradation & restoration (BIA, containment, known good comparison, restoration, restart)
- For market-facing discussions, keep scenarios bounded: prerequisites, stopping points, and sensitivity.



**Next Month:** Tail risk: why OT loss is fat-tailed and why scenario credibility matters. Educational content only. Not legal, coverage, or underwriting advice.

# Consolidated OT Cybersecurity and Cyber Insurance Developments (February 2026)

## Executive summary

This briefing consolidates reputable, publicly reported developments in two adjacent domains during February 2026: (1) operational technology (OT) / industrial control systems (ICS) cybersecurity incidents, advisories, and research; and (2) cyber insurance market and regulatory developments. The scope is intentionally restricted to publications dated in February 2026.

- Incident-driven OT reporting in February was dominated by follow-on analysis and government messaging related to the destructive campaign against Polish energy facilities, including malware analysis and operator guidance (OT 1-5).
- Vulnerability disclosure volume and vendor advisory cadence remained high, with multiple weekly ICS advisory roundups, late-February CISA ICS advisories, and an industry analysis highlighting record advisory counts and high average severity in 2025 (OT 6-10 and 16-18).
- In cyber insurance, strategic activity was notable: market commentary suggested Zurich's bid for Beazley could catalyze additional specialty-line deal activity, reinforcing consolidation dynamics in cyber-specialty underwriting platforms (INS-1).
- Competitive cyber insurance conditions continued to soften with reported rate decreases and expanding capacity, while reinsurance commentary indicated significant pricing softening in cyber aggregate excess-of-loss terms at 1/1 renewals (INS 2-5).
- Regulatory and governance expectations continued to evolve, including public written evidence by the Association of British Insurers on the UK Cyber Security and Resilience Bill and late-February reporting on UK supervisory priorities touching cyber (INS-7; INS-10).

## Scope and Method

Inclusion criteria: (a) publication date in February 2026; (b) relevance to OT/ICS cybersecurity or cyber insurance; (c) publication by a reputable source (major media outlet, recognized industry publication, government body, or established research organization). The document does not add new facts beyond what was reported; analysis is limited to synthesis and implications, clearly separated from the reported items. Each item is mapped to a reference identifier and a full citation in the References section.

## OT / ICS cybersecurity developments (February 2026)

Table 1 summarizes February 2026 OT/ICS cybersecurity developments captured in this compilation. Details follow in the same order.

| REF | DATE | HEADLINE | SOURCE |
|---|---|---|---|
| OT-1 | 2026-02-02 | Poland energy-sector destructive attack: default credentials exploited | SecurityWeek |
| OT-2 | 2026-02-06 | DYNOWIPER malware analysis tied to Poland energy-sector campaign | Elastic Security Labs |
| OT-3 | 2026-02-10 | CISA warning amplified by mainstream cyber press (operator lessons) | Cybersecurity Dive |
| OT-4 | 2026-02-10 | Reporting framing DERs as emerging OT target set (Poland incident context) | CyberScoop |
| OT-5 | 2026-02-12 | Trade-press summary: insecure industrial protocols + prevention guidance | ITPro |
| OT-6 | 2026-02-02 | Weekly ICS advisory roundup (CISA ICS advisories): AV26-074 | Canadian Centre for Cyber Security |
| OT-7 | 2026-02-09 | Weekly ICS advisory roundup (CISA ICS advisories): AV26-102 | Canadian Centre for Cyber Security |
| OT-8 | 2026-02-17 | Weekly ICS advisory roundup (CISA ICS advisories): AV26-134 | Canadian Centre for Cyber Security |
| OT-9 | 2026-02-19 | WaterISAC bulletin referencing CISA ICS advisories (Feb 17 & Feb 19 releases) | WaterISAC |
| OT-10 | 2026-02-19 | ICS vulnerabilities and disclosure trends (record volume; high average severity) | Forescout / Vedere Labs |
| OT-11 | 2026-02-17 | Dragos 2026 Year in Review (new OT threat groups; ransomware impact) | Dragos |
| OT-12 | 2026-02-17 | 2026 ICS security outlook (industry panel synthesis) | SecurityWeek |
| OT-13 | 2026-02-19 | SANS synthesis: takeaways from Dragos report | SANS |
| OT-14 | 2026-02-20 | Legacy LonTalk protocol risk in building management systems | Claroty Team82 |
| OT-15 | 2026-02-09 | Peer-reviewed OT/SCADA detection research (IIoT-enabled SCADA traffic) | Scientific Reports (Nature) |
| OT-16 | 2026-02-24 | CISA ICS Advisory: InSAT MasterSCADA BUK-TS | CISA |
| OT-17 | 2026-02-24 | CISA ICS Advisory: Schneider Electric EcoStruxure Building Operation Workstation | CISA |
| OT-18 | 2026-02-24 | CISA ICS Advisory: Gardyn Home Kit | CISA |
| OT-19 | 2026-02-25 | OTI Impact Score ('Richter Scale' model) introduced for OT cyber incident severity communication (S4x26 coverage) | Dark Reading |

*Table 1. OT/ICS cybersecurity items published in February 2026. Source hyperlinks are provided at the end of this document.*

## Cyber insurance developments (February 2026)

Table 2 summarizes February 2026 cyber insurance market, reinsurance, regulation, and product developments captured in this compilation. Details follow in the same order.

| REF | DATE | HEADLINE | SOURCE |
|---|---|---|---|
| INS-1 | 2026-02-05 | Market view: Zurich/Beazley bid could catalyze more specialty deals | Reuters |
| INS-2 | 2026-02-04 | Marsh Global Insurance Market Index (Q4 2025): cyber rates down globally | Marsh |
| INS-3 | 2026-02-05 | Lockton market update: cyber premiums down; capacity expanding | Lockton |
| INS-4 | 2026-02-03 | WTW: cyber risk look-ahead to 2026 (underwriting themes) | WTW |
| INS-5 | 2026-02-02 | Cyber reinsurance: reported ~32% risk-adjusted rate softening for cyber aggregate XOL at 1/1 | Insurance Business (citing Gallagher Re) |
| INS-6 | 2026-02-04 | Trade-press amplification: cyber fines may not be covered | Insurance Business (UK) |
| INS-7 | 2026-02-05 | UK Cyber Security and Resilience Bill: ABI written evidence (cyber insurance perspective) | UK Parliament (bills) |
| INS-8 | 2026-02-02 | Generali (UK): cyber insurance for IFAs (product/portfolio expansion) | Generali Global Corporate & Commercial |
| INS-9 | 2026-02-19 | Liberty Specialty Markets: launch of cyber line in Italy | Reinsurance News |
| INS-10 | 2026-02-24 | UK FCA: AI and cyber reviews under insurance priorities | The Insurer |
| INS-11 | 2026-02-24 | Claims trend commentary: breach claims down 15%–20% overall; individual events growing in size (Experian) | The Insurer TV |
| INS-12 | 2026-02-25 | Claims data / loss trend: Resilience reports shift toward long-tail losses and data-theft extortion | Insurance Journal |

*Table 2. Cyber insurance items published in February 2026. **Source hyperlinks are provided at the end of this document.***

# Cross-cutting synthesis (OT risk and insurance signals)

February 2026 reporting reinforces a recurring cyber–physical pattern: widely distributed, increasingly integrated, remotely managed industrial environments (including distributed energy resources) make credential hygiene, perimeter defense, and edge device exposure decisive risk drivers. In parallel, the cyber insurance market continues to signal strong competition and expanding capacity; buyers may see improved terms, but carriers will need disciplined risk differentiation (controls, architecture, and recovery posture) to sustain underwriting performance.

Two governance pressures are particularly visible in the month's coverage:

**01.** Public policy and governance expectations around the role of cyber insurance continue to evolve (e.g., written evidence by the Association of British Insurers on the UK Cyber Security and Resilience Bill)

**02.** The market's ability to evidence and price long tail, high severity cyber physical loss scenarios depends on the quality and consistency of OT exposure evidence (asset roles, connectivity, remote access paths, and recovery testing).

These observations synthesize the items listed in Sections 1 and 2 and introduce no additional facts beyond the cited publications.

Additional February publications add two signals relevant to cyber physical risk communication and insurability: (1) the OTI Impact Score concept presented at S4x26 aims to standardize how OT incident severity is communicated to executives and cyber insurers (OT–19), and (2) cyber claims commentary continues to emphasize a shift toward longer tail loss drivers tied to data exposure and downstream legal and regulatory impacts (INS–12).

# Closing the Cyber-Physical Risk Gap

by Neil Arklie *(Head of Insurance Solutions)*
and George Mawdsley *(Head of Risk Solutions)*

Following Neil Arklie 's session at S4x26 in Miami South Beach (Feb 23–26, 2026), DeNexus published a short booklet to help OT asset owners, brokers, insurers, and reinsurers align on a shared challenge: the insurance and capital gap for cyber events that escalate into operational disruption and physical consequences.

Cyber risk in industrial environments has changed shape. As information technology and operational technology become more interconnected, cyber incidents are no longer confined to data or business systems. They can interrupt production, disrupt critical services, and—at the extreme—contribute to physical consequences when control, equipment protection, human safety functions are degraded in a cyber-attack.

The market 's capacity challenge is not a lack of interest; it is a translation challenge. OT teams naturally describe exposure in architectures, vulnerabilities, lack of safeguards, and operational dependencies. Underwriters and reinsurers must translate those realities into underwriting discipline: severity, limit adequacy, aggregation, and capital efficiency. When those views do not align, risk is under-recognized—especially where loss is driven by downtime rather than data theft—limits remain conservative, and a growing share of cyber-physical exposure stays on the asset owner 's balance sheet.

> The booklet grounds this in operational reality. It includes the Jaguar Land Rover incident (August 2025), where an IT compromise led to precautionary shutdowns that propagated across manufacturing and third-party supply chains. All major UK manufacturing plants—Solihull, Halewood, and Wolverhampton—stopped for roughly six weeks, with a reported £1.9bn UK financial impact affecting over 5,000 organizations. The lesson is straightforward: operational dependence can turn a cyber event into a prolonged production halt, and limit adequacy becomes a board-level financial question.

So what closes the gap? The booklet frames the problem as a value-chain requirement. For cyber-physical risk to move from **client → insurer → reinsurer → capital**, downstream markets need three things to allocate capacity with confidence: clear data, scenario models, and aggregation control. When those foundations are credible and consistent, risk becomes legible, portfolios become manageable, and limits can scale responsibly.

## Be first to access the full booklet.

*Launching next week. Click here to opt-in and get the booklet directly to your inbox*

# OT Cyber Incidents Resulting in Property Damage

OT Cyber Incidents Resulting in Property Damage is a DeNexus "field guide to publicly reported cyber-physical loss events and near misses," based on research conducted in June 2025 using publicly available sources.

The analysis draws from "**public databases of disclosed incidents and cybersecurity research,"** and the list is not exhaustive due to data availability. DeNexus notes it does not know whether losses were insured and does not use confidential loss data or infer insurance coverage.

*OT systems govern physical processes; when cyber activity reaches control networks/systems, consequences can extend beyond IT impacts to include equipment damage, fires/explosions, environmental releases, and prolonged business interruption. Even though confirmed malicious OT incidents that directly cause property damage are described as comparatively rare, the guide argues this is not a reason for complacency, because loss can scale quickly when controls, protections, or safety functions are undermined.*

### Patterns that guide highlights across incidents

- Cyber-physical outcomes are driven by physics—once operating limits are violated, the process behaves accordingly, regardless of attacker intent.
- Many pathways begin with traditional IT compromise and become severe after movement into OT and interference with visibility/control/safety.
- Near misses still matter (example referenced: Triton) because "no explosion" can be luck, design, or attacker error—yet the pathway is still credible.

**The guide reports:** 8 malicious OT incidents with property damage involving manipulation of control (over the last 40 years); 4 incidents involving bricking devices; 4 accidental OT cyber incidents with property damage (to understand potential loss magnitude); and 4 other OT-affecting incidents often excluded for different reasons.

The document emphasizes that an attacker doesn't need full plant control—changing a limited set of inputs, outputs, alarms, or VFD parameters can create unsafe conditions. It lists recurring methods: input value manipulation, output manipulation, disabling alarms/shutdowns, and altering VFD parameters, with impacts that can include process deviations (e.g., overfill), operational disruption (spurious trips/delayed response), and equipment damage (overspeed).

It advocates moving beyond qualitative assessments toward financially quantifying expected loss (probability-weighted scenario impacts). This "missing bridge" supports better investment prioritization, stronger business accountability, and more defensible risk transfer/insurance discussions using credible cyber-physical loss estimates.

## Be first to access the full booklet.

*Launching in two weeks. Click here to opt-in and get the booklet directly to your inbox*

# Incident reporting and government advisories

OT-1 — 2026-02-02 —

Poland energy-sector destructive attack: default credentials exploited (SecurityWeek) *Source: https://www.securityweek.com/default-ics-credentials-exploited-in-destructive-attack-on-polish-energy-facilities/*

OT-2 — 2026-02-06 —

DYNOWIPER malware analysis tied to Poland energy-sector campaign (Elastic Security Labs)
*Source: https://www.elastic.co/security-labs/dynowiper*

OT-3 — 2026-02-10 —

CISA warning amplified by mainstream cyber press (operator lessons) (Cybersecurity Dive)
*Source: https://www.cybersecuritydive.com/news/cisa-critical-infrastructure-warning-poland-energy-hack/811819/*

OT-4 — 2026-02-10 —

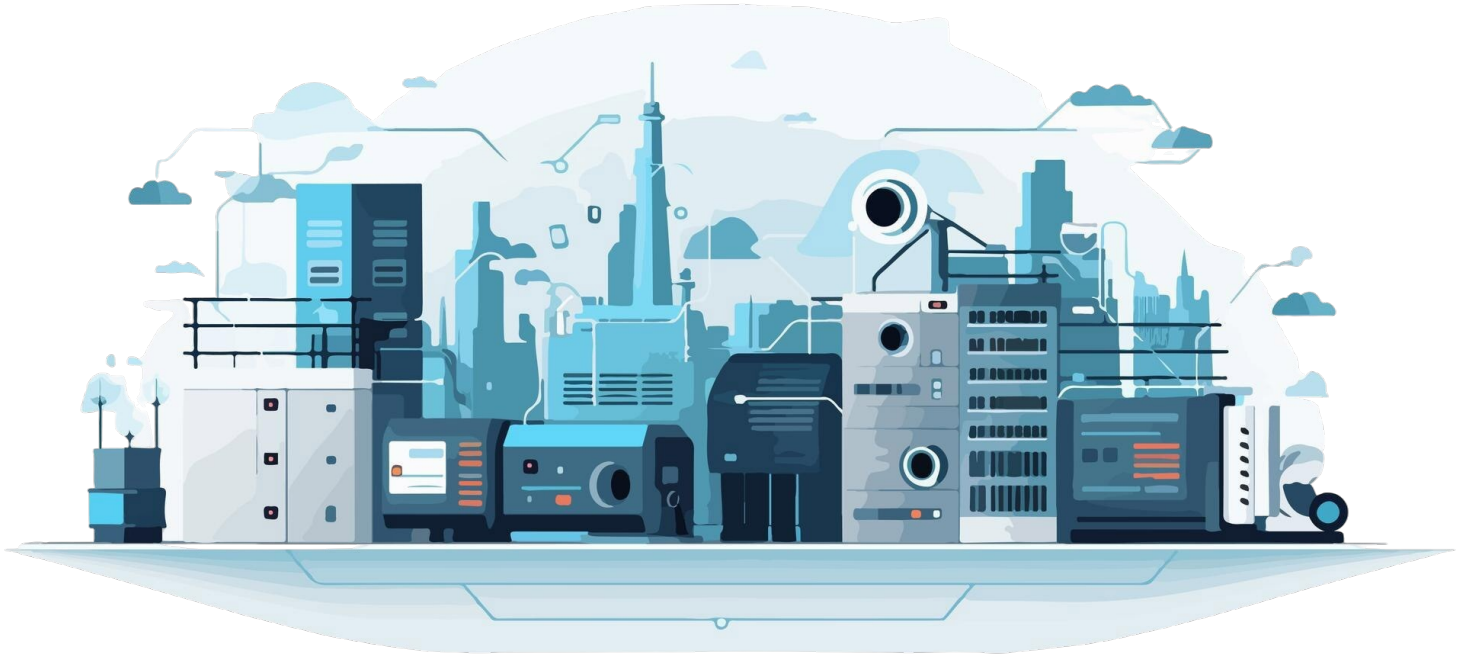
Reporting framing DERs as emerging OT target set (Poland incident context) (CyberScoop)
*Source: https://cyberscoop.com/cisa-warning-russian-cyberattack-poland-power-grid/*

OT-5 — 2026-02-12 —

Trade-press summary: insecure industrial protocols + prevention guidance (ITPro)
*Source: https://www.itpro.com/security/cisa-shares-lessons-learned-from-polish-power-grid-hack-and-how-to-prevent-disaster-striking-again*

OT-5 — 2026-02-12 —

Trade-press summary: insecure industrial protocols + prevention guidance (ITPro)
*Source: https://www.itpro.com/security/cisa-shares-lessons-learned-from-polish-power-grid-hack-and-how-to-prevent-disaster-striking-again*



## Vulnerability advisories and disclosure trends

OT-6 — 2026-02-02 —

Weekly ICS advisory roundup (CISA ICS advisories): AV26-074 (Canadian Centre for Cyber Security)

*Source: https://www.cyber.gc.ca/en/alerts-advisories/control-systems-cisa-ics-security-advisories-av26-074*

OT-7 — 2026-02-09 —

Weekly ICS advisory roundup (CISA ICS advisories): AV26-102 (Canadian Centre for Cyber Security)

*Source: https://www.cyber.gc.ca/en/alerts-advisories/control-systems-cisa-ics-security-advisories-av26-102*

OT-8 — 2026-02-17 —

Weekly ICS advisory roundup (CISA ICS advisories): AV26-134 (Canadian Centre for Cyber Security)

*Source: https://www.cyber.gc.ca/en/alerts-advisories/control-systems-cisa-ics-security-advisories-av26-134*

OT-9 — 2026-02-19 —

WaterISAC bulletin referencing CISA ICS advisories (Feb 17 & Feb 19 releases) (WaterISAC)

*Source: https://www.waterisac.org/tlpclear-cisa-ics-advisories-additional-alerts-updates-and-bulletins-february-19-2026*

OT-10 — 2026-02-19 —

ICS vulnerabilities and disclosure trends (record volume; high average severity) (Forescout / Vedere Labs)

*Source: https://www.forescout.com/blog/ics-cybersecurity-in-2026-vulnerabilities-and-the-path-forward/*

OT-16 — 2026-02-24 —

CISA ICS Advisory: InSAT MasterSCADA BUK-TS (CISA)

*Source: https://www.cisa.gov/news-events/ics-advisories/icsa-26-055-01*

OT-17 — 2026-02-24 —

CISA ICS Advisory: Schneider Electric EcoStruxure Building Operation Workstation (CISA)

*Source: https://www.cisa.gov/news-events/ics-advisories/icsa-26-055-02*

OT-18 — 2026-02-24 —

CISA ICS Advisory: Gardyn Home Kit (CISA)

*Source: https://www.cisa.gov/news-events/ics-advisories/icsa-26-055-03*

## Threat landscape and research publications

OT-11 — 2026-02-17 —

Dragos 2026 Year in Review (new OT threat groups; ransomware impact) (Dragos)

*Source: https://www.dragos.com/resources/press-release/dragos-2026-year-in-review-new-ot-threats-ransomware*

OT-12 — 2026-02-17 —

2026 ICS security outlook (industry panel synthesis) (SecurityWeek)

*Source: https://www.securityweek.com/cyber-insights-2026-the-ongoing-fight-to-secure-industrial-control-systems/*

OT-13 — 2026-02-19 —

SANS synthesis: takeaways from Dragos report (SANS)

*Source: https://www.sans.org/blog/top-takeaways-from-the-dragos-ot-cybersecurity-report-2026*

OT-14 — 2026-02-20 —

Legacy LonTalk protocol risk in building management systems (Claroty Team82)

*Source: https://claroty.com/team82/research/examining-the-legacy-bms-lontalk-protocol*

OT-15 — 2026-02-09 —

Peer-reviewed OT/SCADA detection research (IIoT-enabled SCADA traffic) (Scientific Reports (Nature))

*Source: https://www.nature.com/articles/s41598-026-37146-1*

## OT incident severity communication

OT-19 — 2026-02-25 —

OTI Impact Score ('Richter Scale' model) for OT cyber incident severity communication (Dark Reading)

*Source: https://www.darkreading.com/ics-ot-security/richter-scale-model-measures-cyber-incidents*

## Pricing, Capacity, and Underwriting Cycle

### INS-2 — 2026-02-04 —

Marsh Global Insurance Market Index (Q4 2025): cyber rates down globally (Marsh)

*Source: https://www.marsh.com/en/about/media/global-commercial-insurance-rates-fall-4-percent-in-q4-2025.html*

### INS-3 — 2026-02-05 —

Lockton market update: cyber premiums down; capacity expanding (Lockton)

*Source: https://global.lockton.com/eu/en/news-insights/cyber-insurance-market-update-rates-decline-despite-rising-claims*

### INS-4 — 2026-02-03 —

WTW: cyber risk look-ahead to 2026 (underwriting themes) (WTW)

*Source: https://www.wtwco.com/en-us/insights/2026/02/cyber-risk-a-look-ahead-to-2026*

### INS-11 — 2026-02-24 —

Claims trend commentary: breach claims down 15%–20% overall; individual events growing in size (Experian) (The Insurer TV)

*Source: https://www.theinsurer.com/tv/news-in-focus/breach-claims-down-15-to-20-but-individual-events-growing-exponentially-2026-02-24/*

### INS-12 — 2026-02-25 —

Claims data / loss trend: Resilience reports shift toward long-tail losses and data-theft extortion (Insurance Journal)

*Source: https://www.insurancejournal.com/news/national/2026/02/25/859511.htm*

## Reinsurance

### INS-5 — 2026-02-02 —

Cyber reinsurance: reported ~32% risk-adjusted rate softening for cyber aggregate XOL at 1/1 (Insurance Business (citing Gallagher Re))

*Source: https://www.insurancebusinessmag.com/reinsurance/news/breaking-news/historic-softening-in-cyber-reinsurance-pricing-as-rates-plunge-32--gallagher-re-563874.aspx*

## Coverage issues and insurability (fines, exclusions, and constraints)

INS-6 — 2026-02-04 —

Trade-press amplification: cyber fines may not be covered (Insurance Business (UK))

*Source:https://www.insurancebusinessmag.com/uk/news/cyber/cyber-fines-piling-up-in-emea-but-insurance-may-not-cover-them-564183.aspx*

## Regulation and incident reporting rulemaking

INS-7 — 2026-02 — 05

UK Cyber Security and Resilience Bill: ABI written evidence (cyber insurance perspective) (UK Parliament (bills))

*Source: https://bills.parliament.uk/publications/64807/documents/7803*

INS-10 — 2026-02-24 —

UK FCA: AI and cyber reviews under insurance priorities (The Insurer)

*Source: https://www.theinsurer.com/ti/news/fca-to-launch-ai-and-cyber-reviews-under-insurance-priorities-2026-02-24/*

## Product and distribution moves

INS-8 — 2026-02-02 —

Generali (UK): cyber insurance for IFAs (product/portfolio expansion) (Generali Global Corporate & Commercial)

*Source: https://www.generaliglobalcorporate.com/media/press-releases/all/2026/Generali-strengthens-financial-lines-portfolio-with-cyber-insurance-for-IFAs.html*

INS-9 — 2026-02-19 —

Liberty Specialty Markets: launch of cyber line in Italy (Reinsurance News)

*Source: https://www.reinsurancene.ws/liberty-specialty-markets-launches-energy-construction-and-cyber-in-italy/*