CYBERSOL

CYBERSOL B.V.

BN3

Bad News on 3rd Parties

Monthly Intelligence on Third-Party Cyber Liability

March 2026

56 third-party incidents tracked

Healthcare Supply Chain Exposure | Regulatory Enforcement Escalation | Subcontractor Blind Spots

Cybersol B.V. | The Hague, Netherlands

cybersol.nl

EXECUTIVE SUMMARY

Key Findings

Total Incidents	Sectors Affected	Geographies
56	8	14+

BN3 is Cybersol's monthly intelligence digest tracking third-party incident coverage published on the Cybersol blog. In March 2026, 56 qualifying incidents were tracked across healthcare, financial services, government, energy, manufacturing, and technology sectors spanning at least fourteen countries. Of these, 25 involved ransomware deployment and 31 involved unauthorized data exposure.

Three themes dominated the month. First, healthcare supply chain exposure: the TriZetto breach affected 3.4 million patients, the Conduent investigation reached 25 million records under Texas AG scrutiny, and the Stryker wiper attack disrupted hospital supply chains across continents. Second, regulatory enforcement escalation: Infosys McCamish's $17.5 million settlement established a financial precedent for vendor breach liability, while the Bank of England's PS7/26 formally requires third-party incident reporting as a regulatory obligation. Third, subcontractor blind spots: the ManoMano breach (37.8 million records via a Zendesk subcontractor) and the Ericsson incident (seven-month vendor notification delay) exposed governance gaps at the subcontractor tier that primary vendor due diligence does not reach.

Regulatory posture hardened in March: UK regulators published PS7/26, the Texas AG opened the Conduent investigation, and class action settlements confirmed that downstream enterprises bear full financial liability for vendor security failures.

The pattern across March's 56 incidents is consistent: organizations manage vendor risk at the primary contract level while subcontractors, notification timelines, and liability allocation remain unaddressed. The governance gap is not detection — it is the contractual framework that defines what happens after a vendor fails.

Key Takeaway: Vendor contracts that do not address subcontractor accountability, notification timelines, and liability allocation are governance documentation — not governance.

MONTH AT A GLANCE

March 2026 — By the Numbers

Counts reflect qualifying BN3 incidents, not unique victims or organizations affected.

QUALIFYING INCIDENTS	INVOLVED RANSOMWARE	DATA EXPOSURE
56	**25**	**31**
unique third-party events	44% of total	55% of total

Top Sectors by Incident Count

Sector	Incidents
Healthcare	33
Financial Services	20
Government	2

Incident Types

Type	Count
Data Exposure	31
Ransomware	25

Vendor Dependency Pattern

Pattern	Count
Healthcare IT	26
Software Supply Chain	21
SaaS / Cloud Service	8

METHODOLOGY

How This Report Is Built

Qualification — What counts as a third-party incident

A cybersecurity incident primarily caused by, occurring at, or materially involving an external vendor, partner, or service provider, where impact includes at least one of: data exposure, unauthorized access, service disruption, extortion or ransomware, or formal regulatory disclosure. Generic guides, trend articles, and editorial commentary are excluded.

Duplicate Handling — When the same incident has multiple posts

When multiple Cybersol blog posts cover the same underlying incident from different sources, the earliest or most complete analysis is the primary entry. Additional coverage appears as "Also covered by:" in the Full Index. Primary selection criteria: word count and governance depth.

BN3-R — Highest Regulatory Risk	BN3-P — Greatest Public Impact	BN3-C — Most Preventable
Fines, enforcement actions, consent orders, GDPR/NIS2/DORA/HIPAA violations, class action settlements, cross-border regulatory complications.	Scale of harm: records exposed (700K+), critical infrastructure disruption, government service failures, national media coverage.	Standard governance would have prevented it: unpatched known CVEs, missing out-of-band verification, software supply chain gaps.

SCOPE & LIMITATIONS

Coverage, Exclusions, and Known Constraints

Coverage Window — March 2026

This edition covers third-party cyber incidents published on the Cybersol blog during March 2026. Post publication date approximates reporting date; some underlying incidents may have occurred in prior periods and are counted in the month they were reported. All 56 qualifying incidents are listed in the Full Index.

Exclusions — What is not counted

The following categories are excluded from the incident count: (1) Opinion articles, trend analysis, and editorial commentary without a named incident. (2) Duplicate coverage of the same underlying incident — one primary entry is retained; additional coverage is noted as "Also covered by:" in the Full Index. (3) Incidents where third-party involvement is speculative or unconfirmed in the source post. (4) Vendor advisory and regulatory guidance publications with no associated breach or disruption event.

Known Limitations

BN3 relies entirely on public reporting and Cybersol blog analysis. It does not reflect incidents that were not disclosed, not covered in English-language sources, or fell outside the coverage window. Incident details may evolve after publication; prior editions are not retroactively updated. Counts represent qualifying events, not unique organizations or individuals affected. This report does not constitute legal, regulatory, or professional advice. All trademarks referenced belong to their respective owners.

HIGHEST REGULATORY RISK

BN3-R: Top 3

Fines. Enforcement. Regulatory fallout.

1

Texas Attorney General Investigates 25M+ Conduent Business Services Data Breach

Mar 09 — via HIPAA Journal

The Texas Attorney General opened a formal investigation into the Conduent Business Services data breach affecting more than 25 million records, marking the largest government contractor breach disclosed in 2026 and triggering concurrent HIPAA and state-level notification obligations across multiple covered entities. Under HIPAA, covered entities remain jointly liable for business associate violations regardless of contractual indemnification clauses — a regulatory reality most vendor agreements are not structured to address.

Governance signal: Joint HIPAA liability applies regardless of vendor contract indemnification clauses.

Post

2

Infosys Settles Data Breach Class Action Lawsuits for $17.5M

Mar 19 — via Bank Info Security

Infosys McCamish Systems agreed to a $17.5 million class action settlement following a November 2023 LockBit ransomware attack that exposed data for more than 6 million individuals across insurance and retirement sectors. The settlement establishes a financial precedent: downstream enterprises bear full regulatory and financial liability for vendor security failures, yet vendor contracts rarely allocate accountability proportionally or include enforceable incident response timelines.

Governance signal: Vendor settlement costs now flow to downstream clients — contracts must allocate liability explicitly.

Post

3

PS7/26 – Operational resilience: Operational incident and third-party reporting

Mar 29 — via Bank of England

The Bank of England's Policy Statement 7/26 (March 2026) formally requires financial institutions to classify vendor relationships against regulatory criteria, identify critical third parties, and report material operational incidents involving those vendors within defined timelines. PS7/26 transforms third-party risk management from an internal control discipline into a formal regulatory reporting requirement — boards now have direct accountability for vendor incident classification and disclosure.

Governance signal: Third-party incident reporting is now a regulatory obligation, not an internal control.

Post

Governance lesson: Regulators are establishing that downstream enterprises bear full financial and legal liability for vendor failures. PS7/26, the Conduent investigation, and the Infosys settlement collectively signal that vendor incident reporting and liability allocation are now regulatory requirements.

GREATEST PUBLIC IMPACT

BN3-P: Top 3

Scale. Visibility. Real-world consequences.

1

Zendesk-Linked Contractor Breach Exposes Data of 37.8 Million ManoMano Customers

Mar 29 — via CX Today

Compromised credentials at an unnamed Zendesk subcontractor exposed 37.8 million ManoMano customer records, making it the largest single-vendor breach by record count in March 2026. ManoMano contracted with Zendesk; the breach originated at a subcontractor ManoMano had no direct relationship with — a governance blind spot that existing vendor due diligence frameworks do not systematically address.

Governance signal: Subcontractor credential management must be a contractual obligation, not an assumption.

Post

2

Cognizant TriZetto breach exposes health data of 3.4 million patients

Mar 11 — via Bleeping Computer

Cognizant's TriZetto Provider Solutions disclosed that a breach exposed protected health information for 3.4 million patients across multiple HIPAA-covered entities that relied on TriZetto for eligibility processing. A single eligibility verification vendor serving dozens of health systems created simultaneous HIPAA notification obligations across multiple states — a governance scenario most healthcare vendor risk frameworks are not designed to handle.

Governance signal: Vendor concentration in healthcare eligibility creates multi-jurisdiction HIPAA exposure by default.

Post

3

Stryker Cyberattack Wipes Employee Devices, Handala Claims Breach

Mar 12 — via TechNadu

An Iran-linked threat actor (Handala) deployed wiper malware against Stryker Corporation, allegedly destroying over 200,000 internal systems, exfiltrating 50 terabytes of data, and forcing the closure of nearly 80 offices across multiple continents — directly disrupting hospital surgical supply chains. The attack demonstrated that a single medical device supplier can become a systemic failure point for hospital operations, with downstream impact on patient care timelines that no vendor contract currently addresses.

Governance signal: Medical supply chain resilience requires contractual continuity-of-supply obligations, not just SLAs.

Post

Governance lesson: Healthcare vendor concentration creates systemic patient-impact risk. When a single vendor serves dozens of health systems, the breach impact scales with the vendor's market share, not the breached organization's size. Subcontractor visibility is the critical gap.

MOST PREVENTABLE

BN3-C: Top 3

The gap between knowing and doing.

1

From Trivy to Broad OSS Compromise: TeamPCP Hits Docker Hub, VS Code, PyPI

Mar 29 — via SecurityWeek

The TeamPCP campaign compromised packages across Docker Hub, VS Code Marketplace, and PyPI — including LiteLLM versions 1.82.7 and 1.82.8 — by publishing malicious packages that mimicked legitimate security tooling, turning trusted software delivery channels into attack vectors. Organizations that enforced package signature verification, maintained allowlists for approved open-source dependencies, or monitored for unexpected package publisher changes would have detected the compromise before deployment — standard software supply chain controls that most enterprises have not yet implemented.

Governance signal: OSS package verification and publisher change monitoring are basic controls, not advanced capabilities.

Post

2

Ericsson breach blamed on third party vendor vishing attack

Mar 25 — via The Register

An unnamed third-party vendor of Ericsson fell victim to a vishing (voice phishing) attack that exposed data for 15,661 individuals, but the vendor did not notify Ericsson until seven months after discovering the unauthorized access. The seven-month notification delay — not the initial vishing attack — is the governance failure: a basic contractual requirement for 72-hour vendor breach notification would have contained the exposure window and reduced regulatory liability under GDPR, NIS2, and US state breach laws.

Governance signal: Vendor breach notification SLAs must be contractual, time-bound, and auditable.

Post

3

Marquis says over 672,000 people had personal and financial data stolen in ransomware attack

Mar 24 — via TechCrunch

A ransomware attack on Marquis Software Solutions compromised personal and financial data for 672,075 individuals across more than 80 U.S. banks and credit unions that relied on the fintech vendor for marketing and account management services. The breach exploited a known vulnerability class in the vendor's network infrastructure; standard network segmentation, timely patching, and privileged access controls would have limited or prevented the lateral movement that enabled mass data exfiltration.

Governance signal: Shared fintech vendors require contractual evidence of segmentation and patch cadence, not just SOC 2.

Post

Governance lesson: March's preventable incidents share a common root cause — controls that exist in policy were not applied to the vendor context that failed. Package verification, breach notification SLAs, and network segmentation are solved problems. The gap is contractual enforcement, not technical capability.

COMPLETE INDEX

All Incidents — March 2026

Date	Incident	Source	Link
Mar 05	**Vendor breach may have exposed Bayada client data** *When healthcare provider Bayada Home Health Care disclosed a data breach originating not from its own systems but from third-party vendor Doctor Alliance, it...*	*via Paubox*	Post
Mar 09	**US Healthcare Diagnostic Firm Says 140,000 Affected by Data Breach - SecurityWeek** *Summary withheld (insufficient post detail).*	*via SecurityWeek*	Post
	Also covered by: HealthExec, HealthExec		
Mar 09	**Internal data of Airbus and Boeing supplier is out: What hackers have stolen this time?** *The compromise of LISI Group, a Tier-1 supplier to Airbus and Boeing, by the Qilin ransomware group represents a structural failure in supply chain vendor risk...*	*via Cyber News*	Post
Mar 09	**INC Ransom Claims Breach of ACWA Power and Larsen & Toubro - TechNadu**	*via TechNadu*	Post
Mar 09	**Texas Attorney General Investigates 25M+ Conduent Business Services Data Breach** *Summary withheld (insufficient post detail).*		Post
	Also covered by: Beckerspayer, Malwarebytes, TechCrunch, Malwarebytes, TechCrunch, Wyosupport, TechCrunch, Malwarebytes, Malwarebytes, TechCrunch, Mysanantonio		
Mar 09	**Change Healthcare breach: The cyberattack's impact 2 years later - Modern Healthcare** *Summary withheld (insufficient post detail).*	*via Modern Healthcare*	Post
	Also covered by: Nixonpeabody, Modern Healthcare		
Mar 09	**IU Health files lawsuit against healthcare tech company following 2024 data breach - Indiana Daily Student** *Summary withheld (insufficient post detail).*	*via Indiana Daily Student*	Post
Mar 10	**Major health provider data breach may have affected thousands more people - over 700k now thought to have been hit | TechRadar** *A breach affecting over 700,000 individuals across multiple health provider organizations—originating from TriZetto Provider Solutions, a Cognizant...*	*via TechRadar*	Post

Mar 10	**The Breach Came From a Vendor You Never Hired Third-Party & Supply Chain — Feb 26, 2026 | By Alice Eneyo | by Alice eneyo | Feb, 2026 | Medium** *The June 2025 compromise of Chain IQ Group AG—a procurement platform serving at least 19 direct clients and exposing over 130,000 employee records—illustrates...*	*via Medium*	Post
Mar 10	**Dozens of Major Data Breaches Linked to Single Threat Actor - SecurityWeek** *The concentration of dozens of major data breaches under a single threat actor operating across energy, aerospace, defense, healthcare, and telecommunications...*	*via SecurityWeek*	Post
Mar 10	**Shocking Healthcare Cyberattack: Worldleaks Ransomware Gang Strikes US Drug Manufacturer Sagent Pharmaceuticals - UNDERCODE NEWS** *Summary withheld (insufficient post detail).*		Post
Mar 11	**Hacktivists Claim DHS Breach, Leak 6,600+ ICE Contractor Records** *A claimed hacktivist breach of Department of Homeland Security systems exposing 6,681 ICE contractor applicant records—including personnel from major...*		Post
Mar 11	**Cognizant TriZetto breach exposes health data of 3.4 million patients** *Summary withheld (insufficient post detail).*	*via Bleeping Computer*	Post
	Also covered by: HIPAA Journal, TechCrunch		
Mar 11	**Symantec reports Iranian Seedworm hackers infiltrate US infrastructure and defense supply chain networks - Industrial Cyber** *Iranian state-sponsored actors maintaining persistent access within US defense contractor networks is not primarily a technical incident—it is structural...*		Post
	Also covered by: Security		
Mar 11	**How a Supplier Ransomware Attack Shut Down Toyota's Just-in-Time Manufacturing | OT Cybersecurity** *The ransomware attack on Kojima Industries—a critical Toyota supplier—resulted in the operational shutdown of 14 manufacturing facilities.*	*via Blastwave*	Post
Mar 12	**LexisNexis Breach Exposes Federal Judges and DOJ Attorneys to Hackers - State of Surveillance** *Summary withheld (insufficient post detail).*		Post
	Also covered by: Cyber News, Lawnext, American Banker		

Mar 12	**Stryker Cyberattack Wipes Employee Devices, Handala Claims Breach - TechNadu** *The Stryker Corporation cyberattack—involving alleged wiper malware that destroyed over 200,000 internal systems, exfiltrated 50 terabytes of proprietary data,...*	*via TechNadu*	Post
	Also covered by: Co, The Week, Yahoo, Medicaldevice Net Work, Medium, Substack, The Beltway Report, El Balad, Alltoc, Cnn, Stryker, Upi, Unn, Tildee, Wkzo, J C A, Industrial Cyber, Digitalhealth News, Advancedmanufacturing, Alliant		
Mar 12	**FBI Wiretap Breach: What Happened and Why It Matters** *Summary withheld (insufficient post detail).*		Post
Mar 12	**How a ransomware attack left an Ontario government health agency scrambling | Globalnews.ca** *When a vendor within a critical supply chain experiences a ransomware compromise, the primary organization faces cascading liability, regulatory exposure, and...*	*via Global News*	Post
Mar 12	**ENGlobal Energy Contractor Ransomware Breach and CenterPoint Energy Data Leak** *Summary withheld (insufficient post detail).*	*via Industrial Cyber*	Post
	Also covered by: The Record, The Record, SecurityWeek		
Mar 12	**Pickett USA breach allegedly exposes sensitive engineering data linked to US utilities** *In January 2026, a threat actor publicly offered 139 GB of operational engineering data allegedly stolen from Pickett USA, a Tampa-based firm serving three...*	*via Industrial Cyber*	Post
	Also covered by: Industrial Cyber, Industrial Cyber, Industrial Cyber, The Register		
Mar 13	**Data breach affecting 11 physician practices confirmed to impact 627K patients** *The confirmed compromise of ApolloMD's network infrastructure—affecting 11 physician practices and 627,000 patient records—represents a structural governance...*	*via HealthExec*	Post
Mar 13	**After tax return data leak, US Treasury terminates consulting firm Booz Allen Hamilton contracts - The Times of India** *The US Treasury Department's termination of its contracts with Booz Allen Hamilton—following the 2024 conviction of a former IRS contractor for leaking...*	*via Times of India*	Post
Mar 16	**Ontario health agency vendor suffered major ransomware attack in 2025 | Globalnews.ca** *When a third-party vendor to a public health organization suffers a ransomware attack involving personal health information, the incident becomes a test of...*	*via Global News*	Post

	Also covered by: Global News		
Mar 17	**Vendor Ransomware Incident Exposes Patient Data Linked to Vikor Scientific - HIPAA Coach** *Summary withheld (insufficient post detail).*	*via HIPAA Coach*	Post
Mar 18	**Third-party vendors drive 45% of breaches in US energy sector** *Third-party vendors account for nearly half of all confirmed breaches in US energy infrastructure, with forensic evidence suggesting they drive 90% of...*		Post
Mar 18	**Major US Banks Gauge Their Exposure to SitusAMC Breach** *Summary withheld (insufficient post detail).*		Post
	Also covered by: SecurityWeek		
Mar 18	**Bank of America customer data exposed in IT provider breach** *When 57,028 Bank of America customer records—including Social Security numbers and addresses—were compromised through Infosys McCamish Systems in November...*		Post
Mar 19	**Infosys Settles Data Breach Class Action Lawsuits for $17.5M** *Summary withheld (insufficient post detail).*	*via Bank Info Security*	Post
Mar 24	**Interlock ransomware gang exploited Cisco firewall zero-day weeks before disclosure: Amazon | The Record from Recorded Future News** *The Interlock ransomware group's exploitation of CVE-2026-20131 in Cisco Secure Firewall Management Center—beginning January 26, weeks before public disclosure...*	*via The Record*	Post
Mar 24	**A Potential Breach of an Anonymous Tip App Could Have Exposed Sensitive Student Data**	*via Education Week*	Post
Mar 24	**[AKIRA] - Ransomware Victim: bdtronic - RedPacket Security** *The alleged AKIRA ransomware compromise of BDTRONIC—a German manufacturing vendor serving automotive, electronics, telecommunications, and renewable energy...*		Post
Mar 24	**Marquis says over 672,000 people had personal and financial data stolen in ransomware attack | TechCrunch** *Summary withheld (insufficient post detail).*	*via TechCrunch*	Post
	Also covered by: Bank Info Security, Bank Info Security, SC World, American Banker, Sbs Cyber, SC World, The Record, SecurityWeek, Sbs Cyber, Bleeping Computer		

Mar 24	**$5.25M Cadence Bank Settlement Ends Class Action Lawsuit Over May 2023 Data Breach** *Summary withheld (insufficient post detail).*		Post
Mar 24	**Bain Struggles to Dismiss PowerSchool User Data Breach Claims** *The failure of Bain Capital and PowerSchool to dismiss data breach claims affecting approximately 50 million individuals—students, parents, and...*	*via Bloomberg Law*	Post
	Also covered by: Pro Skauer, Labaton		
Mar 25	**Crunchyroll Data Breach Exposes 100GB Of User Data — How A Single Compromised Vendor Unlocked Sony's Crown Jewels + Video - Undercode Testing** *Summary withheld (insufficient post detail).*		Post
	Also covered by: TechRepublic		
Mar 25	**Ericsson breach blamed on third party vendor vishing attack**		Post
	Also covered by: Prism News, 5Gstore, The Register, Crn, Red Packet Security, Infosecurity Magazine, Bleeping Computer, The Register, Bleeping Computer, The Register, Bleeping Computer		
Mar 26	**Deaconess patients' sensitive data stolen in vendor breach - DataBreaches.Net** *The Deaconess Health System breach—in which a third-party medical records vendor was compromised, exposing patient information across two hospitals—is not...*	*via DataBreaches.net*	Post
	Also covered by: Beckershospital Review, Satpr Wire		
Mar 26	**CommonSpirit Health Patients Affected by Vendor Data Breach** *Summary withheld (insufficient post detail).*	*via HIPAA Journal*	Post
Mar 26	**When a Cyberattack Hits a National Champion: The £1.5 Billion Bailout That Exposed Britain's Missing Playbook** *Summary withheld (insufficient post detail).*	*via Web Pro News*	Post
Mar 27	**[AKIRA] - Ransomware Victim: Autitransa - RedPacket Security** *Summary withheld (insufficient post detail).*		Post
Mar 27	**Hackerone Slams Supplier For Delayed Breach Notice After Staff Data Exposed - RedPacket Security** *The breach at Navia Benefit Solutions affecting nearly 300 HackerOne employees illustrates a critical structural failure in third-party breach notification...*	*via Red Packet Security*	Post
	Also covered by: The Register		

Mar 27	**California-based semiconductor testing company reports ransomware attack to SEC | The Record from Recorded Future News** *When a vendor files a breach disclosure with the SEC, downstream customers often assume they will be notified through formal channels.*	*via The Record*	Post
Mar 27	**Palm Bay Portal Down: BridgePay Ransomware Attack** *Summary withheld (insufficient post detail).*	*via The Palm Bayer*	Post
Mar 29	**Zendesk-Linked Contractor Breach Exposes Data of 37.8 Million ManoMano Customers** *Summary withheld (insufficient post detail).*	*via CX Today*	Post
	Also covered by: CX Today, Cpo Magazine, CX Today		
Mar 29	**From Trivy to Broad OSS Compromise: TeamPCP Hits Docker Hub, VS Code, PyPI - SecurityWeek** *Summary withheld (insufficient post detail).*	*via SecurityWeek*	Post
Mar 29	**Bend La-Pine Schools: 'SeeSaw' security breach led to app removal from iPads** *Summary withheld (insufficient post detail).*	*via Central Oregon Daily*	Post
Mar 29	**PS7/26 – Operational resilience: Operational incident and third-party reporting | Bank of England** *The Bank of England's Policy Statement 7/26 (March 2026) transforms third-party risk management from an internal control discipline into a formal regulatory...*	*via Bank of England*	Post
	Also covered by: Digit, Infosecurity Magazine, Org, Financialinstitutions News, Org		
Mar 29	**[PLAY] - Ransomware Victim: TPIS Industrial Services - RedPacket Security** *When a ransomware group publicly claims to have compromised an industrial supplier—even without corroborating evidence—downstream customers and regulatory...*	*via Red Packet Security*	Post
Mar 29	**Thousands of Corewell Health patients affected by 2024 vendor data breach | FOX 2 Detroit** *Summary withheld (insufficient post detail).*	*via FOX 2 Detroit*	Post
	Also covered by: Detroit News, Hoodline		
Mar 29	**[PAYLOAD] - Ransomware Victim: A A Al Moosa Enterprises (ARENCO Group) - RedPacket Security** *Ransomware incident reporting has become a critical input to vendor risk assessment, regulatory compliance workflows, and insurance underwriting.*	*via Red Packet Security*	Post

Mar 29	**Sensitive patient health information leaked in Texas third-party software breach | FOX 4 Dallas-Fort Worth** *The Doctor Alliance breach—affecting Amedisys, Angels Care Home Health, and Accent Care—is not primarily a technical failure.*	*via FOX 4*	Post
Mar 30	**[AKIRA] - Ransomware Victim: Dixon Electrical Systems & Contracting - RedPacket Security** *The reported AKIRA ransomware incident targeting Dixon Electrical Systems & Contracting—a full-service electrical contractor serving industrial and...*	*via Red Packet Security*	Post
Mar 30	**Worcester's emergency notification system back online after breach - masslive.com** *Worcester's emergency notification system breach—originating from third-party provider OnSolve CodeRED in November 2025—is not a technology incident.*	*via MassLive*	Post
Mar 31	**[NIGHTSPIRE] - Ransomware Victim: JT-ATFP, LLC - RedPacket Security** *The reported compromise of JT-ATFP, LLC by NIGHTSPIRE ransomware—involving exfiltration of classified contracts, employee records, and Department of Defense...*	*via Red Packet Security*	Post
Mar 31	**NYC Health Notifying Patients of 2 Third-Party Hacks** *New York City Health + Hospitals' notification of two separate third-party breaches—one affecting 90,000 patients through a care management partner, another...*	*via GovInfoSecurity*	Post
	Also covered by: HealthExec		

CYBERSOL NEWS

Cybersol News

Cybersol Selected for ImpactCity Grants for Impact 2026

March 27, 2026

Cybersol B.V. was selected as one of seven startups for the ImpactCity Grants for Impact 2026 programme, receiving advisory support for the company's work in EU cyber governance and supply chain security serving regulated organizations.

Post

Cybersol Announces Open-Source Release of GOSTA

March 27, 2026

Cybersol released GOSTA, an open-source specification for governing autonomous AI agent decision-making. The framework defines decision authority, operational boundaries, and failure protocols — addressing governance gaps in current AI agent tooling.

Post

DDD Featured as "New Innovation" in Security Delta's March Security Insight

March 13, 2026

Security Delta (HSD) recognized Cybersol's Design Driven Development framework as a "New Innovation" in their March 2026 newsletter, alongside contributions from Fox-IT, KPN, and Booz Allen Hamilton.

Post

ABOUT CYBERSOL

Governance Infrastructure for Post-Breach Accountability

Cybersol builds governance infrastructure for post-breach accountability — the operational gap between detection and compliance where notification requirements, obligation tracking, and liability documentation are managed.

OBLIGO — Cyber Liability Operating System

Want to discuss third-party liability governance?

cybersol.nl | LinkedIn: Cybersol B.V. | X: @Cybersolbv

HSD — The Hague Security Delta Premium Partner