CYBERSOL

CYBERSOL B.V.

BN3

Bad News on 3rd Parties

Monthly Intelligence on Third-Party Cyber Liability

February 2026

78 third-party incidents tracked

Vendor Concentration | Regulatory Hardening | Preventable Failures

Cybersol B.V. | The Hague, Netherlands

cybersol.nl

EXECUTIVE SUMMARY

Key Findings

Total Incidents	Sectors Affected	Geographies
78	7	12+

BN3 is Cybersol's monthly intelligence digest tracking third-party incident coverage published on the Cybersol blog. In February 2026, 78 qualifying incidents were tracked across financial services, healthcare, government, education, and critical infrastructure sectors in at least twelve countries. Of these, 21 involved ransomware deployment and 48 involved unauthorized data exposure.

Three themes dominated the month. First, vendor concentration risk: single providers — TriZetto in healthcare eligibility, Conduent in government IT, Marquis Software in financial services — generated cascading failures across dozens of downstream organizations simultaneously. Second, regulatory hardening: the FTC's 10-year consent orders against Illuminate Education and Illusory Systems signal that documented remediation processes are no longer optional — failure to act on identified vulnerabilities is now an independent basis for enforcement. Third, preventable failures: the Warlock ransomware breach via an unpatched SmarterMail server, a six-month Notepad++ supply chain compromise, and a $4.9M business email compromise at a North Dakota school district all resulted from the absence of basic controls.

Regulatory posture tightened across jurisdictions: NYDFS issued clarifying guidance on third-party cybersecurity expectations, and FTC enforcement against education-sector vendors established that vulnerability-discovery-without-remediation constitutes inadequate governance.

The pattern that emerges from February's incident set is consistent: organizations are investing in detection while underinvesting in the contractual and operational frameworks that define what happens when a vendor fails. Remediation accountability — who is obligated to act, by when, and with what documentation — remains the governance gap.

Key Takeaway: Vendor failure is a recurring operational risk; the governance question is whether your contracts specify what happens next.

MONTH AT A GLANCE

February 2026 — By the Numbers

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

QUALIFYING INCIDENTS	INVOLVED RANSOMWARE	DATA EXPOSURE
78	**21**	**48**
unique third-party events	26% of total	61% of total

Top Sectors by Incident Count

Sector	Incidents
Healthcare	20
Technology / Other	18
Financial Services	17

Incident Types

Type	Count
Data Exposure	48
Ransomware	21
BEC / Fraud	8

Vendor Dependency Pattern

Pattern	Count
General Third Party	53
Software Supply Chain	13
Payment Processor	6

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 — February 2026

This edition covers third-party cyber incidents published on the Cybersol blog during February 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 78 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

FTC Announces 10-Year Information Security Consent Orders with Illuminate Education and Illusory Systems

Feb 26 — via Inside Privacy

The FTC imposed 10-year information security consent orders on Illuminate Education and Illusory Systems after both organizations failed to act on vulnerabilities identified through third-party processes, exposing student data across multiple school districts. The enforcement action signals that regulators now treat failure to remediate third-party-identified vulnerabilities — not just the breach itself — as an independent basis for sustained regulatory intervention.

Governance signal: Documented remediation timelines are now a regulatory requirement, not best practice.

Post

2

How a Firewall Zero-Day Turned a Vendor Breach Into a Banking-Sector Event

Feb 18 — via Security Buzz

A ransomware attack on Marquis Software Solutions — enabled by exploitable SonicWall firewall vulnerabilities — compromised data across more than 80 U.S. banks and credit unions, affecting 824,000 consumers and triggering a regulatory notification avalanche. The resulting lawsuit against SonicWall challenges the industry assumption that vendors bear minimal liability once a product is sold, with direct implications for how financial institutions structure vendor contracts and allocate security risk.

Governance signal: Vendor liability clauses must address product vulnerability disclosure, not just service delivery.

Post

3

Conduent Data Breach: Timeline and What to Know

Feb 19 — via Security Magazine

A ransomware incident at Conduent, a major IT services provider to public-sector organizations, disrupted government benefit payment systems and triggered mandatory breach notifications across multiple states and client organizations. The incident illustrates how a single outsourced IT provider can become a systemic failure point for government services, with cascading regulatory notification obligations that exceed what individual client risk frameworks are designed to handle.

Governance signal: Concentration risk in outsourced government IT requires contractual notification SLAs.

Post

Governance lesson: Regulators are moving from breach-response to breach-prevention accountability. Documented vendor vulnerability remediation processes — with timelines and ownership — are now a regulatory expectation, not a best practice.

GREATEST PUBLIC IMPACT

BN3-P: Top 3

Scale. Visibility. Real-world consequences.

1

Thousands More Learn Their Health Info Stolen from TriZetto

Feb 24 — via The Register

TriZetto Provider Solutions disclosed that a 2024 data incident exposed healthcare eligibility records for more than 3.6 million individuals across multiple HIPAA-covered entities, with the exposure going undetected for months. A single eligibility verification vendor serving dozens of health systems created overlapping HIPAA notification obligations across multiple states simultaneously — 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

2

Illinois Department of Human Services Data Breach Affects 700K People

Feb 26 — via Cybersecurity Dive

A third-party vendor incident affecting the Illinois Department of Human Services exposed personal data of approximately 700,000 residents who depend on state-administered public assistance programs. The breach demonstrates that public-sector vendor governance gaps carry disproportionate social impact: the individuals affected have limited ability to opt out of the data relationships that made them vulnerable.

Governance signal: Government vendor contracts must include enforceable security standards, not just data processing terms.

Post

3

Betterment Data Breach Exposes 1.4 Million Customers

Feb 20 — via American Banker

Threat group ShinyHunters accessed Betterment customer data for 1.4 million accounts by targeting third-party platforms — specifically Salesforce systems used by the digital wealth management provider — rather than Betterment's own infrastructure. The incident illustrates a persistent governance gap: organizations invest heavily in securing their own perimeter while third-party SaaS platforms holding equivalent data are subject to minimal contractual security requirements.

Governance signal: SaaS vendor security obligations must match the sensitivity of data held, not the vendor category.

Post

Governance lesson: Vendor concentration creates amplified public harm. When a single provider fails, the impact is not proportional to one organization — it is proportional to every organization that depended on that vendor. Risk frameworks must account for shared dependencies.

MOST PREVENTABLE

BN3-C: Top 3

The gap between knowing and doing.

1

Warlock Ransomware Breaches SmarterTools Through Unpatched SmarterMail Server

Feb 20 — via Bleeping Computer

The Warlock ransomware group breached SmarterTools by exploiting documented vulnerabilities in an unpatched SmarterMail server deployment, compromising the company's own email infrastructure and potentially exposing downstream clients. The attack required no novel technique: a publicly known vulnerability, an unpatched server, and sufficient dwell time to deploy ransomware — a failure sequence that patch cadence and basic vulnerability management would have interrupted.

Governance signal: Patch management must cover internally deployed vendor software, not just third-party SaaS.

Post

2

Notepad++ Compromised for 6 Months: Check Your Version Now

Feb 19 — via Cyber Desserts

The Notepad++ open-source text editor, used by millions of developers globally, was compromised at the distribution level for approximately six months before detection, with trojanized versions serving as an unmonitored attack vector into developer environments. Organizations that tracked installed software versions and validated cryptographic signatures of development tools would have detected the anomaly; most did not, because developer tooling sits outside standard vendor risk and software asset management processes.

Governance signal: Developer tooling must be included in software supply chain monitoring and version control.

Post

3

North Dakota School District Scammed Out of Almost $5 Million

Feb 19 — via KFGO

Dickinson Public Schools in North Dakota lost approximately $4.92 million to a business email compromise attack in which fraudsters impersonated a vendor and redirected two construction project payments to fraudulent accounts. The fraud required no technical sophistication: a spoofed email, a missing out-of-band verification step, and an absence of dual-authorization controls for large payment changes to vendor banking details were sufficient to redirect nearly $5 million.

Governance signal: Vendor payment changes above a threshold require out-of-band callback verification, always.

Post

Governance lesson: February’s preventable incidents share a common root cause — controls that existed elsewhere in the organization were not applied to the specific context that failed. Patch management, software inventory, and payment verification are solved problems. The gap is scope, not capability.

COMPLETE INDEX

All Incidents — February 2026

Date	Incident	Source	Link
Feb 18	**How a Firewall Zero-Day Turned a Vendor Breach Into a Banking-Sector Event - Security Buzz** *Summary withheld (insufficient post detail).*	*via Security Buzz*	Post
	Also covered by: Web Pro News, TechCrunch, The Lyon Firm, Digitrendz, American Banker, Blueshift		
Feb 18	**Cyber Attack Disrupts Local Government Payment Systems** *The recent ransomware attack on BridgePay Network Solutions has sent shockwaves through the public sector, disrupting payment processing systems for multiple...*	*via Gov Tech*	Post
Feb 18	**BTU restores credit card payments after vendor ransomware attack** *When residents of Bryan, Texas attempted to pay their utility bills with credit or debit cards in early February 2026, they encountered an unexpected obstacle.*	*via KBTX*	Post
Feb 19	**Bayada Home Health Care Affected by Doctor Alliance Data Breach** *When Bayada Home Health Care, a major healthcare provider operating across 22 states, announced that patient data had been compromised through their...*	*via HIPAA Journal*	Post
Feb 19	**Key Apple, Nvidia, and Tesla supplier sees confidential files allegedly exposed in major breach - here's what we know so far | TechRadar** *Summary withheld (insufficient post detail).*		Post
	Also covered by: Yahoo, Gadget Hacks, Infosecurity Buzz, iPhone in Canada, Hackread, Mynymbox		
Feb 19	**Notepad++ Compromised for 6 Months: Check Your Version Now** *When cybersecurity professionals assess third-party risks, they typically focus on enterprise software vendors, cloud service providers, and managed service...*	*via Cyber Desserts*	Post
Feb 19	**Conduent Data Breach: Timeline and What to Know | Security Magazine** *Summary withheld (insufficient post detail).*	*via Security Magazine*	Post

Feb 19	**Adapt Integrated Health Care reports data breach at vendor, assures patient info safety** *The healthcare industry's increasing reliance on third-party vendors for critical functions like electronic medical records processing has created a complex...*		Post
Feb 19	**North Dakota school district scammed out of almost $5 million | The Mighty 790 KFGO | KFGO** *A sophisticated email fraud scheme has cost a North Dakota school district nearly $5 million, exposing critical vulnerabilities that extend far beyond a single...*	*via KFGO*	Post
	Also covered by: The Dickinson Press, InForum, Gov Tech		
Feb 19	**Pell City School System data breached by cyber attack** *Summary withheld (insufficient post detail).*		Post
Feb 19	**New Research: 64% of 3rd-Party Applications Access Sensitive Data Without Justification** *Summary withheld (insufficient post detail).*	*via The Hacker News*	Post
Feb 20	**Nearly 17,000 Volvo staff dinged in supplier breach • The Register** *Summary withheld (insufficient post detail).*	*via The Register*	Post
	Also covered by: Red Packet Security		
Feb 20	**Warlock Ransomware Breaches SmarterTools Through Unpatched SmarterMail Server** *Summary withheld (insufficient post detail).*	*via The Hacker News*	Post
Feb 20	**Mexican Government Data Breach: Legacy Systems and Third-Party Vendor Risks Exposed** *When a data breach strikes a government agency, the immediate focus typically centers on firewalls, intrusion detection systems, and internal security...*	*via Kiteworks*	Post
Feb 20	**Data breach hits University of Phoenix via Oracle vulnerability | Fox News** *Summary withheld (insufficient post detail).*	*via Fox News*	Post
Feb 20	**Betterment data breach exposes 1.4 million customers | American Banker** *Summary withheld (insufficient post detail).*		Post
Feb 20	**Data breach hits 1 million Figure customers | American Banker** *Summary withheld (insufficient post detail).*	*via American Banker*	Post

Feb 20	**Hackers claim breach of engineering firm, offer sale of info on three major US utilities | TechRadar** *The cybersecurity community has long warned about third-party risk, but a recent breach targeting Pickett and Associates—an engineering firm serving major U.S.*	*via TechRadar*	Post
Feb 20	**Pickett USA breach allegedly exposes sensitive engineering data linked to US utilities - Industrial Cyber** *Summary withheld (insufficient post detail).*	*via Industrial Cyber*	Post
	Also covered by: SC World, The Register		
Feb 20	**Hackers Breach Engineering Firm, Threaten Sale of Utility Info | SSOJet News Central - Breaking Boundaries. Building Tomorrow** *The recent cyberattack on Pickett USA, an engineering services firm serving major utility companies, has exposed a vulnerability that keeps security executives...*	*via Ssojet*	Post
Feb 21	**PRIVACY ALERT: TriZetto Provider Solutions Under Investigation for Data Breach of Over 700,000 Patient Records** *The investigation into TriZetto Provider Solutions' breach affecting over 700,000 patient records reveals a structural governance vulnerability that extends...*	*via PR Newswire*	Post
Feb 21	**Ransomware surge in 2025 exposes mounting OT risk as industrial impacts outpace IT narratives - Industrial Cyber** *Summary withheld (insufficient post detail).*	*via Industrial Cyber*	Post
Feb 21	**[Expert Opinion] Gallo Fall: \"Reclaiming Senegal's digital sovereignty after the DAF cyberattack** *Summary withheld (insufficient post detail).*	*via Seneweb*	Post
	Also covered by: Seneweb		
Feb 21	**San Diego Unified School District Settlement Class Action Over Data Breach** *Summary withheld (insufficient post detail).*	*via Class Action*	Post
Feb 23	**Ambulance Billing Vendor Reaches Settlement With Connecticut Over Data Breach | Across Connecticut, CT Patch** *Summary withheld (insufficient post detail).*	*via Patch*	Post
Feb 24	**THE KNOWNSEC LEAK: Yet Another Leak of China's Contractor-Driven Cyber-Espionage Ecosystem - DomainTools Investigations | DTI** *The KnownSec data leak, documented by DomainTools Investigations, exposes a structural vulnerability in how organizations assess vendor risk: the inability to...*	*via DomainTools*	Post

Feb 24	**Stalkerware vendor data breach exposes over half a million customer records | SC Media** *Summary withheld (insufficient post detail).*	*via SC World*	Post
Feb 24	**Thousands more learn their health info stolen from TriZetto • The Register**	*via The Register*	Post
	Also covered by: HealthExec, HIPAA Journal, Paubox, MercyOne		
Feb 24	**Third-Party Cyber Risk: Why Vendor Attacks Are Rising and How Organizations Can Respond | CyberMaxx** *Summary withheld (insufficient post detail).*	*via Cyber Maxx*	Post
Feb 24	**Treasury rips up Booz Allen contracts after Trump tax data leak - InvestmentNews** *Summary withheld (insufficient post detail).*	*via Investment News*	Post
Feb 24	**NYDFS Clarifies Expectations For Third-party Cybersecurity Risk Management - Security - United States** *The New York Department of Financial Services' recent clarifying letter on third-party cybersecurity risk management represents a critical inflection point in...*	*via Mondaq*	Post
Feb 24	**[NITROGEN] - Ransomware Victim: DeWalch Technologies, Inc - RedPacket Security** *Summary withheld (insufficient post detail).*	*via Red Packet Security*	Post
Feb 24	**235K members of Minnesota-based credit union notified of data breach after cyberattack** *Summary withheld (insufficient post detail).*	*via Star Tribune*	Post
Feb 25	**Hackers breach contractor linked to Ukraine's central bank collectible coin store | The Record from Recorded Future News** *The breach of a contractor serving Ukraine's National Bank—reportedly exploited as an entry point to target the institution itself—exposes a fundamental...*		Post
Feb 25	**Vikor Scientific Affected by Ransomware Attack on Revenue Cycle Management Vendor**	*via HIPAA Journal*	Post
Feb 25	**Jupiter Medical alerts patients after third party data breach exposes health records** *Summary withheld (insufficient post detail).*	*via Cbs12*	Post
Feb 25	**Leading Japanese semiconductor supplier responding to ransomware attack | The Record from Recorded Future News** *A ransomware attack on Advantest, a leading Japanese semiconductor test equipment manufacturer, is not a localized incident.*	*via The Record*	Post

Feb 25	**Key Apple supplier suffers data breach that could expose confidential product files - 9to5Mac** *Summary withheld (insufficient post detail).*	*via 9to5Mac*	Post
Feb 25	**Discord Zendesk breach highlights growing risk of third-party vendor access | ThreatLocker Blog** *Summary withheld (insufficient post detail).*	*via Threatlocker*	Post
Feb 25	**Spanish electricity company Endesa reports customer data theft, including bank details | Sur in English** *When a major European critical infrastructure provider experiences a data breach involving financial identifiers and customer contract details, the incident...*	*via Sur in English*	Post
	Also covered by: The Register, SecurityWeek		
Feb 25	**Cyber Vendor Evaluation That Protects Your Business from Vendor Breaches | The AI Journal** *Summary withheld (insufficient post detail).*	*via Aijourn*	Post
Feb 25	**[THEGENTLEMEN] - Ransomware Victim: Intsika Yethu Municipality Government - RedPacket Security** *Summary withheld (insufficient post detail).*	*via Red Packet Security*	Post
Feb 26	**Munson, Hagerty The Latest Traverse City Organizations Hit By Major Data Breaches | The Ticker** *Summary withheld (insufficient post detail).*	*via Traverseticker*	Post
Feb 26	**TowneBank Vendor Data Breach | Website Cyber Security ■■** *Summary withheld (insufficient post detail).*	*via Website Cyber*	Post
Feb 26	**Marietta unable to process online payments due to ransomware attack – WSB-TV Channel 2 - Atlanta** *The City of Marietta's operational paralysis following the BridgePay Network Solutions ransomware attack is not a technology incident—it is a governance...*	*via Wsbtv*	Post
Feb 26	**Illinois Department of Human Services data breach affects 700K people** *When a state agency, university, and major telecommunications provider experience significant data breaches within the same reporting window—collectively...*	*via Bleeping Computer*	Post
Feb 26	**FTC Announces 10-Year Information Security Consent Orders with Illuminate Education and Illusory Systems | Inside Privacy** *The Federal Trade Commission's 10-year information security consent orders against Illuminate Education and Illusory Systems reveal a structural governance...*	*via Inside Privacy*	Post

Feb 27	**TriZetto Provider Solutions Issues Data Breach Notifications to HIPAA Covered Entities (Update)** *When a single healthcare technology vendor experiences a security breach, the resulting notification obligations do not remain contained within that vendor's...*	*via HIPAA Journal*	Post
Feb 27	**Health insurance tech provider TriZetto says more than 3 million impacted by 2024 breach | The Record from Recorded Future News** *Summary withheld (insufficient post detail).*	*via The Record*	Post
Feb 27	**PowerSchool, Chicago Schools Agree to Pay $17.25M Settlement** *The $17.25M settlement between PowerSchool and Chicago Public Schools represents a critical failure in third-party data stewardship that extends far beyond a...*	*via Gov Tech*	Post
Feb 27	**EEOC experienced security incident involving contractor's 'unauthorized' access, email says - Nextgov/FCW** *Summary withheld (insufficient post detail).*	*via Nextgov*	Post
Feb 27	**Europe's ManoMano Hit: 38M Customer Records Compromised in Vendor Breach** *The compromise of 38 million customer records through a third-party customer service vendor represents a structural failure in vendor risk governance that...*	*via TechRepublic*	Post
Feb 27	**Conduent Data Breach Becomes Largest in U.S. History After Ransomware Group Steals 8 TB** *The Conduent ransomware incident—resulting in the theft of 8 TB of sensitive government payment and healthcare data—represents a critical failure point in...*	*via Cyber Press*	Post
Feb 27	**Ransomware cyberattack hits City of Bloomington payment vendor | WGLT** *When a critical payment processing...*	*via Wglt*	Post
Feb 28	**Marquis Software Breach Reaches Blaze Credit Union As Vendor Fallout Widens Across Industry / Fresh Today / CUToday.info - CU Today** *The breach at Marquis Software—a marketing and compliance vendor serving hundreds of financial institutions—exposed personal information for over 235,000...*	*via CUToday*	Post
Feb 28	**Sedgwick confirms breach at government contractor subsidiary** *When Sedgwick Government Solutions—a federal contractor subsidiary of the larger claims administration firm Sedgwick—suffered a confirmed security breach, it...*	*via Bleeping Computer*	Post

Feb 28	**Wichita online water payment vendor hit by ransomware attack. Here’s how to pay your bill** *Summary withheld (insufficient post detail).*	*via Kansas*	Post
Feb 28	**Credit card payments unavailable for BTU customers following third-party vendor’s ransomware incident** *Summary withheld (insufficient post detail).*	*via KBTX*	Post
Feb 28	**Nearly 57 Million Records Exposed: What the Biggest Health Care Breaches of 2025 Reveal About Today’s Cyber Risk - ACA International** *Summary withheld (insufficient post detail).*	*via ACA International*	Post
Feb 28	**When Your Vendor’s Vendor Gets Breached | VISO TRUST** *When a vendor's sub-contractor experiences a security incident, organizations often discover their third-party risk management frameworks lack the structural...*	*via Visotrust*	Post
Feb 28	**Payment tech provider for Texas, Florida governments working with FBI to resolve ransomware attack | The Record from Recorded Future News** *The ransomware attack on BridgePay Network Solutions—a payment technology provider serving Texas and Florida government operations—represents a structural...*	*via The Record*	Post
Feb 28	**DomainTools Investigations | THE KNOWNSEC LEAK: Yet Another Leak of China’s Contractor-Driven Cyber-Espionage Ecosystem** *Summary withheld (insufficient post detail).*	*via DomainTools*	Post
Feb 28	**Marquis Vendor Breach Reaches 1st MidAmerica Credit Union / Fresh Today / CUToday.info - CU Today**	*via CUToday*	Post
Feb 28	**Associated Wholesale Grocers Beats Second Suit Over 2023 Breach** *When Associated Wholesale Grocers defeated a second proposed class action lawsuit over its 2023 data breach, the legal victory may have signaled procedural...*	*via Bloomberg Law*	Post
Feb 28	**Largest Healthcare Data Breaches of 2025** *Summary withheld (insufficient post detail).*	*via HIPAA Journal*	Post
Feb 28	**r/msp on Reddit: I need Cyber Liability Insurance for my MSP company as my client just got ransomwared and now everyone's asking** *When a managed service provider's client experiences a ransomware incident, the resulting scramble for cyber liability insurance reveals a systemic governance...*	*via Reddit*	Post

Feb 28	**Healthcare breaches double as shadow AI, vendor risks proliferate | Cybersecurity Dive** *Summary withheld (insufficient post detail).*	*via Cybersecurity Dive*	Post
Feb 28	**80 Hospitals May Have Been Affected by the Oracle Health Data Breach** *Summary withheld (insufficient post detail).*	*via HIPAA Journal*	Post
Feb 28	**Canada Goose Data Breach Exposes 600,000 Customers: Inside the Luxury Brand's Cybersecurity Crisis** *Summary withheld (insufficient post detail).*	*via One News Page*	Post
Feb 28	**Notice of Security Incident Involving Third-Party Vendor | ENT & Allergy of Delaware** *The security incident involving ENT & Allergy of Delaware and their third-party vendor TriZetto illustrates a structural governance blind spot that extends...*	*via ENT & Allergy*	Post
Feb 28	**More Than 100K Munson Healthcare Patients Affected by Cerner Cyberattack** *The January 2025 cyberattack on Oracle Health (formerly Cerner), affecting over 100,000 patients across Munson Healthcare and numerous other health systems,...*	*via HIPAA Journal*	Post
Feb 28	**Ransomware group breached SmarterTools via flaw in its SmarterMail deployment - Help Net Security** *Summary withheld (insufficient post detail).*	*via Help Net Security*	Post
Feb 28	**Atlas Air attackers warn Boeing intellectual property at risk in suspected supply chain hack** *Summary withheld (insufficient post detail).*	*via Cyber News*	Post
Feb 28	**Cybersecurity terms in third-party contracts: Are you being served, or served up? | Opinion | Compliance Week** *Third-party cybersecurity contract terms reveal a fundamental governance asymmetry that organizations routinely overlook: standard vendor agreements prioritize...*	*via Compliance Week*	Post
Feb 28	**Healthcare Technology Company Discloses Ransomware Attack**	*via HIPAA Journal*	Post
Feb 28	**The Breach Wasn't Yours—But the Fallout Is | Gavin** *When a vendor or service provider experiences a cyber incident, the breach itself may originate outside your organization—but the regulatory, contractual, and...*	*via Evolving Influence*	Post
Feb 28	**Staten Island University Hospital Settles Lawsuit Over Business Associate Data Breach** *The Staten Island University Hospital settlement over a January 2024 breach at vendor The Medibase Group Inc.*	*via HIPAA Journal*	Post

Feb 28	**Managed Care Advisors/Sedgwick Government Solutions Data Breach Lawsuit - Class Action U** *A data breach at Managed Care Advisors/Sedgwick Government Solutions—a federal government contractor managing workers' compensation and health administration...*	*via Class Action U*	Post

CYBERSOL NEWS

Cybersol News

Cybersol Open-Sources Design Driven Development

February 2026

Cybersol publicly released Design Driven Development (DDD) as open-source under the MIT license — a methodology and toolset for visually designing software and implementing it with AI assistance. The release addresses a recognized gap in AI-assisted development: loss of architectural context between sessions.

Post

Cybersol B.V. Joins Security Delta (HSD) as Premium Partner

February 24, 2026

Cybersol B.V. joined Security Delta (HSD) as a Premium Partner in February 2026, gaining access to the Dutch national cybersecurity ecosystem based in The Hague. The partnership supports engagement with the Dutch market across innovation, capital, and talent networks.

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