CYBERSOL

CYBERSOL B.V.

BN3

Bad News on 3rd Parties

Monthly Intelligence on Third-Party Cyber Liability

May 2026

54 third-party incidents tracked

Single vendors, cascading liability

Detection latency now carries the fine

Patch, payment, AI: basics still fail

Cybersol B.V. | The Hague, Netherlands

cybersol.nl

Prepared by: Cybersol Editorial Desk | Report: BN3 / May 2026 | Version: v1.0 | Generated: 2026-06-01 | Classification: Public (media-derived)

EXECUTIVE SUMMARY

Key Findings

Total Incidents	Sectors Affected	Geographies
54	4	14+

BN3 is Cybersol's monthly intelligence digest tracking third-party cyber incidents from public reporting. The May 2026 edition covers 54 qualifying incidents, with healthcare and financial services accounting for the largest classified-sector share. Of these, 16 involved ransomware deployment and 37 involved unauthorized data exposure.

Three themes dominated. First, single-vendor concentration produced sector-wide cascades: ShinyHunters' Instructure Canvas breach exposed 275 million users across 9,000 educational institutions including 44 Dutch schools, and ChipSoft's ransomware affected a vendor serving roughly 80% of Dutch hospitals. Second, regulators moved from breach severity toward detection and notification latency as an enforcement target — the UK ICO levied a £1 million+ fine against a water utility for a multi-year Cl0p incident, citing dwell time as standalone regulatory liability. Third, basic preventable controls kept failing — cPanel's CVE-2026-41940 was weaponized within 24 hours despite available patches; Pine Bluff School District lost $3.2 million to wire-fraud injection that out-of-band callback verification would have stopped; and a US community bank disclosed customer SSNs uploaded to an unauthorized AI chatbot.

Regulators issued enforcement actions, congressional inquiries, and formal notifications tied to vendor breaches this month; NIS2 and DORA were increasingly cited in litigation against principals, not only vendors.

NYC Health + Hospitals' four-month dwell time before disclosing biometric data on 1.8 million people, combined with the ICO's dwell-time framing, signals that vendor monitoring and contractual notification clauses are moving from advisory to enforceable.

Key Takeaway: Vendor notification obligation is no longer a compliance line item — it is a contractual control that determines whether detection latency becomes liability.

MONTH AT A GLANCE

May 2026 — By the Numbers

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

QUALIFYING INCIDENTS	INVOLVED RANSOMWARE	DATA EXPOSURE
54	**16**	**37**
unique third-party events	29% of total	68% of total

Top Sectors by Incident Count

Sector	Incidents
Healthcare	36
Financial Services	15
Government	2

Incident Types

Type	Count
Data Exposure	37
Ransomware	16
Other	1

Vendor Dependency Pattern

Pattern	Count
Healthcare IT	28
SaaS / Cloud Service	16
Software Supply Chain	9

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 — May 2026

This edition covers third-party cyber incidents published on the Cybersol blog during May 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 54 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

British Privacy Watchdog Fines Water Supplier $1.3 Million Over a Multi-Year Data Breach

May 29 — via Cpo Magazine

The UK Information Commissioner's Office levied a £1 million+ fine against a water utility after Cl0p exfiltrated 4.1TB between May and July 2022, with stolen data later published when ransom demands went unmet. ICO treated detection and notification latency as a standalone regulatory liability, signaling that vendor incident response speed — not only breach severity — now carries enforcement weight for critical-infrastructure suppliers.

Governance signal: Notification Latency: dwell time is now a standalone fineable liability

Post

2

Customers sue Citizens, Frost over third-party data breach

May 07 — via American Banker

Six class action lawsuits were filed against Citizens Bank and Frost Bank after a statement-printing and tax document vendor breach exposed 3.4 million Citizens customer records and over 250,000 Frost Social Security numbers. Plaintiffs are naming the banks — not the vendor — as negligent parties, a framing that aligns emerging case law with NIS2 and DORA continuous-oversight obligations; neither bank has filed a material SEC cybersecurity disclosure.

Governance signal: Direct Liability: contractual separation no longer shields financial institutions

Post

3

CISA GitHub Data Leak 2026: A Nightwing Contractor Exposed AWS GovCloud Keys, Plaintext Passwords, and CISA's DevSecOps Secrets for Six Months

May 23 — via The Tech Marketer

A Nightwing contractor maintained CISA AWS GovCloud keys, plaintext passwords, and DevSecOps secrets in a public GitHub repository for six months, with detection mechanisms reportedly disabled on the contractor side. Lawmakers have demanded answers, and the case demonstrates that regulatory authority and technical sophistication do not guarantee vendor risk management — NIS2 third-party supply-chain provisions and DORA outsourcing-governance frameworks are positioned to apply.

Governance signal: Contractor Accountability: detection controls cannot be left to the vendor

Post

Governance lesson: April's regulatory actions treat absent risk analyses, vendor SEC disclosures, and ambiguous contractor liability as standalone enforcement triggers. The HHS OCR $1.7M settlement, CareCloud's SEC Item 1.05 filing, and the Booz Allen tax-data suit collectively shift accountability from the breach itself to pre-incident documentation and contractual specificity.

GREATEST PUBLIC IMPACT

BN3-P: Top 3

Scale. Visibility. Real-world consequences.

1

ShinyHunters breach Instructure Canvas LMS, claim 275M users and 3.65TB of student data from 9,000 schools including 44 Dutch institutions

May 13 — via The Nextweb

ShinyHunters compromised Instructure's Canvas LMS, claiming 275 million user records and 3.65TB of student data spanning 9,000 educational institutions including 44 Dutch schools and universities. This is Instructure's second major breach by the same actor in eight months, concentrating sensitive student data under a single vendor whose security posture has been repeatedly compromised — with GDPR, NIS2, and FERPA notification obligations cascading to every affected institution.

Governance signal: Vendor Concentration: one edtech vendor's breach cascades to 9,000 institutions

Post

2

Foxconn confirms cyberattack hit some North American factories — hackers say they stole 8TB of data, including Apple and Nvidia files

May 18 — via TechRadar

Foxconn confirmed a cyberattack affecting North American facilities; the Nitrogen ransomware group claimed theft of 8TB of data allegedly including technical files from Apple, Nvidia, Intel, Google, and Dell. A single manufacturing vendor holding competitive technical data for multiple tier-one tech firms turns one breach into a cascading liability event, with NIS2 and DORA reporting obligations and product-liability exposure extending across every named downstream customer.

Governance signal: Multi-Tenant Manufacturing: one vendor breach exposes five competing customers simultaneously

Post

3

NYC Health + Hospitals says hackers stole medical data and fingerprints during breach affecting at least 1.8 million people

May 24 — via TechCrunch

NYC Health + Hospitals — the largest US public hospital system — disclosed that an unnamed vendor breach exposed medical data and fingerprints of at least 1.8 million people, with the compromise persisting undetected from November 2025 through February 2026. The four-month dwell time at a vendor handling biometric and protected health data exposes a fundamental vendor-monitoring gap, with HIPAA notification obligations, NY SHIELD Act scrutiny, and biometric-data regulatory frameworks all now in play.

Governance signal: Vendor Monitoring: four-month dwell time turns biometric exposure into liability

Post

Governance lesson: April's largest cascades — PowerSchool across 62 million students, ChipSoft across 70–80% of Dutch hospitals, and Itron across 7,700 utilities — are concentration-risk events, not localized breaches. Single-vendor dependencies are now systemic-resilience exposures that NIS2 and DORA treat as discrete risk categories.

MOST PREVENTABLE

BN3-C: Top 3

The gap between knowing and doing.

1

cPanel CVE-2026-41940 Exploited Within 24 Hours, Ransomware Deployed

May 11 — via Daily Security Review

cPanel CVE-2026-41940 — an authentication bypass vulnerability — was weaponized within 24 hours of disclosure, with ransomware deployed against managed service providers, government agencies, and military infrastructure in five countries. Patches were available before exploitation, making this a vendor-disclosure-to-customer-patch chain failure rather than a zero-day; organizations relying on cPanel face NIS2 reporting obligations and downstream customer-breach liability for every hour the patch sat undeployed.

Governance signal: Patch Latency: 24-hour weaponization broke the customer patch chain

Post

2

Pine Bluff School District scammed out of more than $3.2 million after cybersecurity hack

May 06 — via Katv

Pine Bluff School District lost $3.2 million in December 2025 (disclosed April 2026) after an attacker compromised an internal employee email account and injected fraudulent wire-transfer instructions into legitimate vendor correspondence. Standard segregated payment controls — out-of-band callback verification for vendor banking changes and dual-authorization on wire transfers — would have stopped the attack at the authorization layer; the loss reveals vendor risk and financial controls operating as disconnected silos.

Governance signal: Payment Verification: out-of-band callback on vendor banking changes is non-negotiable

Post

3

US bank discloses security lapse after sharing customer data with AI app

May 18 — via TechCrunch

Community Bank disclosed a security lapse after an employee uploaded customer names, dates of birth, and Social Security numbers to an unauthorized external AI chatbot. The incident sits between vendor risk management and employee access controls — a gap most organizations have not yet addressed — and would have been prevented by outbound data-loss prevention, an enforced AI usage policy, or restricted egress for sensitive data fields.

Governance signal: AI Usage Policy: employee-initiated uploads need outbound DLP, not awareness training

Post

Governance lesson: April's preventable incidents trace to basic, well-known controls left unapplied — DLP and rate-limiting at the BPO supporting Adobe, out-of-band payment-instruction verification at Pine Bluff, and atomic credential rotation across the Trivy and LiteLLM OSS chain. The technical solutions exist; the contractual obligation to apply them does not.

COMPLETE INDEX

All Incidents — May 2026

Date	Incident	Source	Link
May 06	**Medtronic Confirms Data Breach After ShinyHunters Claims - Infosecurity Magazine** *Medtronic's confirmed data breach affecting 9+ million corporate records presents a critical governance test that extends far beyond the vendor itself.*	*via Infosecurity Magazine*	Post
May 06	**Sandhills Medical Says Ransomware Breach Affects 170,000 - SecurityWeek** *The Sandhills Medical Foundation ransomware incident—affecting 170,000 individuals and discovered May 8, 2025—is not merely a healthcare security failure.*	*via SecurityWeek*	Post
May 06	**Pine Bluff School District scammed out of more than $3.2 million after cybersecurity hack** *Summary withheld (insufficient post detail).*	*via Katv*	Post
May 06	**American Utility Firm Itron Discloses Breach of Internal IT Network** *Summary withheld (insufficient post detail).*	*via Hendryadrian*	Post
	Also covered by: Simplywall, SecurityWeek, TechCrunch		
May 06	**Payload Ransomware Strikes Rural Municipality of Gimli** *Summary withheld (insufficient post detail).*	*via Dexpose*	Post
May 06	**[PAYOUTSKING] - Ransomware Victim: SunSource - RedPacket Security** *When a critical supply chain vendor appears on a ransomware leak page—even without confirmation—the liability and notification burden does not rest with the...*	*via Red Packet Security*	Post
May 07	**Customers sue Citizens, Frost over third-party data breach | American Banker** *Six class action lawsuits filed against Citizens Bank and Frost Bank following a third-party vendor data breach represent a structural shift in how courts and...*		Post
	Also covered by: Computer Bilities, American Banker, American Banker		
May 07	**[FULCRUMSEC] - Ransomware Victim: Woundtech - RedPacket Security** *Summary withheld (insufficient post detail).*		Post

May 07	**CMS Statement on Continued Action to Respond to the Cyberattack on Change Healthcare | CMS** *When the Centers for Medicare & Medicaid Services (CMS) must issue emergency directives for accelerated payments, advance funding, and clearinghouse...*		Post
	Also covered by: Wchsb		
May 07	**As NYC pushes AI in schools, audit finds data breaches, gaps in city data privacy policies** *The New York City Department of Education's failure to maintain centralized visibility over third-party software vendors represents a structural governance...*	*via Chalkbeat*	Post
	Also covered by: Ny Daily News, Hanfordsentinel		
May 08	**[THEGENTLEMEN] - Ransomware Victim: Riggotts - RedPacket Security** *The reported THEGENTLEMEN ransomware incident targeting Riggotts—a UK-based surface coating and line marking contractor—illustrates a critical structural...*	*via Red Packet Security*	Post
May 08	**Trump Administration Inadvertently Exposed Healthcare Providers' Social Security Numbers in Publicly Accessible Database | Congressman John Larson** *When a federal healthcare administration system inadvertently exposes personally identifiable information of thousands of healthcare providers, the incident...*	*via House*	Post
May 08	**Vimeo confirms breach via third-party vendor impacts 119K users** *The Vimeo breach via Anodot—affecting 119,000 users through a third-party analytics vendor compromise by the ShinyHunters group—illustrates a structural...*	*via Security Affairs*	Post
	Also covered by: Co		
May 08	**Hamilton City Hall Discloses Sixth Privacy Breach in Three Years** *Hamilton City Hall's disclosure of a sixth privacy breach within three years—involving volunteer applicant data exposed through a third-party vendor portal...*		Post
May 08	**Bend La-Pine Schools: 'SeeSaw' security breach led to app removal from iPads | Central-oregon-daily | centraloregondaily.com** *The Bend-La Pine Schools' removal of SeeSaw following a vendor security incident illustrates a critical structural vulnerability in how educational...*	*via Central Oregon Daily*	Post
May 08	**Sysco listed on Qilin ransomware leak site with May 12th deadline** *Summary withheld (insufficient post detail).*	*via Cyber News*	Post

May 08	**CareCloud Breach Shows EHR Risk Is Now a Governance Test - HIT Leaders and News** *The CareCloud incident disclosed in May 2026 should not be read as another vendor breach story.*	*via Hitleaders*	Post
May 08	**RXNT Notifies Customers About Cybersecurity Incident and Data Breach** *When a healthcare EHR vendor experiences a breach, the liability and notification burden cascade across dozens or hundreds of downstream healthcare...*	*via HIPAA Journal*	Post
	Also covered by: Security Boulevard		
May 11	**Healthcare Firm Suffers Major Data Breach – Personal, Medical and Health Records of 143,842 People at Risk - The Daily Hodl** *When Innovative Scientific Solutions disclosed a breach affecting 143,842 individuals' personal, medical, and health records, the incident revealed far more...*	*via Daily Hodl*	Post
May 11	**Ransomware Group Takes Credit for Trellix Hack - SecurityWeek** *When a cybersecurity vendor itself becomes a breach victim, the governance implications extend far beyond the compromised organization.*		Post
May 11	**Vendor Says Daemon Tools Supply Chain Attack Contained - SecurityWeek** *Summary withheld (insufficient post detail).*		Post
May 11	**Dutch healthcare software vendor goes dark after ransomware attack** *On April 7, 2026, ChipSoft—a Dutch healthcare software vendor serving approximately 80 percent of the country's hospitals—fell victim to a ransomware attack...*		Post
May 11	**April data breach may have impacted all NC schools; student & staff data accessed :: WRAL.com** *The Canvas/Instructure incident affecting all North Carolina public schools reveals a structural failure in vendor risk management across educational...*	*via Wral*	Post
May 11	**Several Oregon School Districts Warn Families About Data Breach Involving Online Learning Platform - KXL** *The Instructure Canvas breach affecting multiple Oregon school districts illustrates a critical structural vulnerability in educational institution vendor...*		Post
May 11	**Public school data breach may impact many: what we know | CMG Plus** *Summary withheld (insufficient post detail).*		Post

	Also covered by: Rockfmtriangle, Wptf, 961Bbb		
May 11	**cPanel CVE-2026-41940 Exploited Within 24 Hours, Ransomware Deployed - Cybersecurity** *The exploitation of cPanel CVE-2026-41940 within 24 hours across managed service providers, government agencies, and military infrastructure in five countries...*	*via Daily Security Review*	Post
	Also covered by: Msspalert		
May 13	**ShinyHunters breach Instructure Canvas LMS, claim 275M users and 3.65TB of student data from 9,000 schools including 44 Dutch institutions** *The ShinyHunters breach of Instructure Canvas LMS—affecting 275 million users across 9,000 educational institutions, including 44 Dutch schools and...*	*via The Nextweb*	Post
	Also covered by: Fox9, Dark Reading, Education Week, Krebs on Security, Purpleshield Security, Insidehighered, K12Dive, Charlotteobserver, Abc News, Cherwell, Salina Post, Uva, Foxreno, Ksat, Kval, Witn, DataBreaches.net, Districtadministration, Nbc16, Nbcnewyork, Khou, Abc13, DataBreaches.net, Fox5Atlanta, Malwarebytes, Nbcchicago, Abc13, News Day, Kutv, Business Daily Net Work, Wptf, Reuters, Spiceworks, Chalmers, Edu, News 3Lv, Kptv, Pv Times, Fox5Dc, Krebs on Security, Fox5Atlanta, Koin, 6Abc, Tribune Ledger News, K12Dive, State of Surveillance, Malwarebytes		
May 14	**Ericsson US Data Breach Exposes Sensitive Information** *The Ericsson US breach—triggered by a compromised external service provider and exposing personally identifiable information for over 15,000...*	*via Seimless*	Post
May 15	**Austin ISD, UT face cyberattack against software vendor | TPR** *The Instructure breach affecting Austin ISD and UT Austin represents a structural failure in third-party risk management that extends far beyond IT operations.*	*via Tpr*	Post
	Also covered by: Kut		
May 18	**Middle GA schools provide updates after nationwide cyberattack. What we know** *Summary withheld (insufficient post detail).*	*via Macon*	Post
	Also covered by: Aol, Aol		
May 18	**Worldwide data breach involved Charlotte-Mecklenburg Schools information** *The Instructure Canvas breach affecting Charlotte-Mecklenburg Schools and approximately 9,000 educational institutions worldwide exposes a structural...*	*via Wbtv*	Post
	Also covered by: Wccbcharlotte		

May 18	**US bank discloses security lapse after sharing customer data with AI app | TechCrunch** *The Community Bank incident—in which an employee uploaded customer names, dates of birth, and Social Security numbers to an unauthorized external AI...*	*via TechCrunch*	Post
May 18	**DragonForce Ransomware Leveraged in MSP Attack Using RMM Tool - Infosecurity Magazine** *Summary withheld (insufficient post detail).*		Post
May 18	**Liberty Mutual Policyholder Data Dumped After Everest Ransomware Deadline Passes - State of Surveillance** *The May 2026 Liberty Mutual breach—108 GB of policyholder data published by the Everest ransomware group after a missed extortion deadline—represents a...*	*via State of Surveillance*	Post
May 18	**Foxconn confirms cyberattack hit some North American factories — hackers say they stole 8TB of data, including Apple and Nvidia files | TechRadar** *The Foxconn ransomware incident represents a structural failure in third-party vendor risk governance that extends far beyond a single manufacturer's incident...*	*via TechRadar*	Post
	Also covered by: Pymnts, Undercode News, Mac Daily News, TechRepublic, Macobserver, Cloud News, Substack, The Register, Macrumors, Tech Times, 9to5Mac, Hngn, Cybersecurity Dive, Siliconrepublic, Ad Hoc News, Iclarified, News Bytesapp, Co		
May 19	**Uncertainty remains following data breach; Washington County education patrons reminded to stay alert | News | stgeorgeutah.com** *Summary withheld (insufficient post detail).*		Post
May 19	**Scope Systems hack sends Australian mining companies scrambling after cyberattack** *Summary withheld (insufficient post detail).*	*via Afr*	Post
May 19	**Pennsylvania supplier West Pharmaceutical says cyberattack disrupted global operations** *West Pharmaceutical Services' May 4 cyberattack—affecting a global supplier of packaging and drug delivery systems to the pharmaceutical and biotechnology...*	*via Dysruptionhub*	Post
	Also covered by: Gurufocus		
May 20	**Notification: Vendor Cybersecurity Incident - San Diego Unified School District** *When a school district issues a vendor cybersecurity incident notification, it signals a breakdown in pre-incident vendor risk governance.*	*via Sandiegounified*	Post

May 20	**Local impact: How were area schools affected by hack of widely used educational platform? | rocketcitynow.com** *Summary withheld (insufficient post detail).*		Post
May 20	**LBUSD, Cal State, LBCC grading platform hacked in apparent ransomware attack • Long Beach Post News** *When a single vendor's infrastructure is compromised, the impact does not stop at the vendor's door.*	*via Lb Post*	Post
May 20	**Atrium Health affected by Oracle Health breach** *Summary withheld (insufficient post detail).*	*via Beckershospital Review*	Post
	Also covered by: Msn, Charlotteobserver, HIPAA Journal		
May 21	**[INCRANSOM] - Ransomware Victim: Calsoft Inc - RedPacket Security** *When a technology vendor is named in a ransomware claim—verified or not—the structural governance implications ripple across customers, boards, and regulators.*	*via Red Packet Security*	Post
May 23	**CISA GitHub Data Leak 2026: A Nightwing Contractor Exposed AWS GovCloud Keys, Plaintext Passwords, and CISA's DevSecOps Secrets for Six Months** *When a federal cybersecurity agency's own contractor maintains exposed credentials in public repositories for six months—and deliberately disables detection...*	*via The Tech Marketer*	Post
	Also covered by: TechRadar, Tech Loy, Fiduciary Tech, Krebs on Security, Tech Dirt		
May 23	**NATO defense supplier Thales confirms data breach | Cybernews** *When Thales Group—a NATO-linked defense supplier managing identity infrastructure and cryptographic systems across European governments—confirms a data breach,...*	*via Cyber News*	Post
May 24	**Roanoke school division reconsidering online platform after recent data breach - Cardinal News** *Summary withheld (insufficient post detail).*	*via Cardinal News*	Post
May 24	**NYC Health + Hospitals says hackers stole medical data and fingerprints during breach affecting at least 1.8 million people | TechCrunch** *The NYC Health+Hospitals breach—affecting 1.8 million individuals across the largest US public health system—represents a critical failure in third-party...*	*via TechCrunch*	Post
	Also covered by: TechCrunch, Daily Mail, Security Boulevard, Biometricupdate, TechCrunch, Malwarebytes, The Nextweb		

May 29	**British Privacy Watchdog Fines Water Supplier $1.3 Million Over a Multi-Year Data Breach - CPO Magazine** *The UK Information Commissioner's Office enforcement action against a water utility—resulting in a £1 million+ fine for a multi-year ransomware...*	*via Cpo Magazine*	Post
	Also covered by: Co		
May 29	**Be prepared': Expert warns of more Iranian-linked cyberattacks after Stryker hack** *Summary withheld (insufficient post detail).*	*via Wwmt*	Post
May 29	**Data breach exposes information of 22,500 Connecticut Medicaid patients** *The Gainwell Technologies breach affecting 22,500 Connecticut Medicaid beneficiaries through Hartford HealthCare's provider portal exemplifies a critical...*	*via Wfsb*	Post
May 29	**Naturgy Data Leak: What Happened and What It Teaches Us About Third-Party Cyber Risk** *Summary withheld (insufficient post detail).*	*via Cyber Leveling*	Post
May 29	**Software developer breaches town website for resident data, urges better cyber-security - Barrie News** *A municipality's reliance on third-party software platforms for critical resident services—parking permits, personal data collection—creates a contractual and...*	*via Barrietoday*	Post
May 29	**Oncology Institute Data Breach 2026: Third-Party Vendor Compromise Exposes Patient Data in Kroll-Administered Systems – Rescana** *The Oncology Institute breach—disclosed via SEC Form 8-K in May 2026 following unauthorized access to patient data through Kroll-administered third-party...*	*via Rescana*	Post
	Also covered by: SC World, HIPAA Journal		
May 29	**Minnesota Agency Notifies 304,000 of Vendor Breach** *Summary withheld (insufficient post detail).*	*via GovInfoSecurity*	Post

CYBERSOL NEWS

Cybersol News

BN3 — April 2026 edition published

May 4, 2026

Cybersol published the April 2026 BN3 edition on the Cybersol blog, covering 170 qualifying third-party cyber incidents from public reporting. The release is part of the monthly BN3 intelligence digest documenting vendor breach patterns and governance signals.

Post

Cybersol Premium Partner at Security Delta (HSD)

Standing — since February 2026

Cybersol B.V. is a Premium Partner of Security Delta (HSD), The Hague's cybersecurity ecosystem. The partnership supports Cybersol's work on governance infrastructure for third-party cyber liability, including OBLIGO.

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