CYBERSOL

CYBERSOL B.V.

BN3

Bad News on 3rd Parties

Monthly Intelligence on Third-Party Cyber Liability

April 2026

170 third-party incidents tracked

Healthcare vendor concentration

Open-source supply chain weaponized

Risk analysis becomes enforcement

Cybersol B.V. | The Hague, Netherlands

cybersol.nl

EXECUTIVE SUMMARY

Key Findings

Total Incidents	Sectors Affected	Geographies
170	7	14+

BN3 is Cybersol's monthly intelligence digest tracking third-party cyber incidents from public reporting. In April 2026, 170 qualifying incidents were tracked, dominated by healthcare and financial services; 58 involved ransomware and 108 involved unauthorized data exposure.

Three themes dominated the month. First, healthcare vendor concentration produced the largest cascades — TriZetto (Cognizant) reportedly exposed 3.4 million patient records after an 11-month detection gap; ChipSoft ransomware disabled the EHR platform underpinning 70–80% of Dutch hospitals; and CareCloud filed an SEC disclosure for an EHR intrusion affecting 40,000+ healthcare providers. Second, software supply chain attacks moved from theory to active monetization: TeamPCP compromised Trivy and LiteLLM, then announced a Vect ransomware affiliate partnership on BreachForums. Third, payment-instruction fraud through legitimate vendor channels continued to drain public-sector budgets — Pine Bluff School District lost $3.2 million via a compromised email thread.

Regulatory posture hardened: HHS OCR levied $1.7 million in HIPAA fines against four firms for absent risk analyses; Texas sued PowerSchool over the K-12 SIS breach; and Nigeria's NDPC opened simultaneous investigations into Remita and Sterling Bank.

The recurring governance gap is contractual: vendor agreements that do not bind concentration risk, atomic credential rotation, or out-of-band payment verification leave operators directly exposed to NIS2 and DORA enforcement.

Key Takeaway: Vendor notification obligations and concentration risk are now enforceable expectations under HIPAA, NIS2, and DORA — contracts that fail to specify them carry direct regulatory and litigation exposure.

MONTH AT A GLANCE

April 2026 — By the Numbers

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

QUALIFYING INCIDENTS	INVOLVED RANSOMWARE	DATA EXPOSURE
170	**58**	**108**
unique third-party events	34% of total	63% of total

Top Sectors by Incident Count

Sector	Incidents
Healthcare	81
Financial Services	61
Government	12

Incident Types

Type	Count
Data Exposure	108
Ransomware	58
Other	3

Vendor Dependency Pattern

Pattern	Count
Healthcare IT	66
SaaS / Cloud Service	61
Software Supply Chain	37

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 — April 2026

This edition covers third-party cyber incidents published on the Cybersol blog during April 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 170 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

Poor Risk Analysis Cost 4 Firms $1.7 Million in HIPAA Fines

Apr 30 — via GovInfoSecurity

HHS OCR fined four healthcare organizations a combined $1.7 million for inadequate HIPAA security risk analyses, with related ransomware incidents reportedly affecting roughly 427,000 individuals. The settlements include two-year monitoring and corrective-action plans, and one defendant — Consociate Health — is a third-party benefits administrator, signaling that vendor-side risk-analysis gaps now carry direct enforcement exposure.

Governance signal: Document risk analyses; absent assessments are themselves a Security Rule violation.

Post

2

Cloud-Based EHR Vendor Notifies SEC About Hacking Incident

Apr 06 — via Bank Info Security

CareCloud, an EHR vendor serving over 40,000 healthcare providers across all 50 states, disclosed a March 2026 hacking incident to the SEC after attackers accessed one of its six EHR environments for eight hours. The filing reflects SEC Item 1.05 cyber-disclosure obligations and creates a notification cascade for downstream covered entities, who reportedly remained dependent on vendor forensics to meet their own HIPAA, state AG, and emerging NIS2 timelines.

Governance signal: Vendor SEC disclosures trigger downstream HIPAA notification clocks for every customer.

Post

3

Trump, IRS Ask for Pause in $10 Billion Suit Over Tax Data Leak

Apr 30 — via Bloombergtax

The $10 billion class action stemming from the Booz Allen Hamilton tax-data exfiltration — for which former contractor employee Charles Littlejohn is reportedly serving a five-year sentence — was placed on hold at the request of the Trump administration and the IRS. The litigation reportedly tests whether "industry-standard" contractual controls are sufficient when authorized vendor users move bulk sensitive data, with direct implications for NIS2 Article 17 supply-chain clauses and DORA Article 16 ICT third-party risk requirements.

Governance signal: Contractually mandate insider-behavior monitoring and bulk-export controls for privileged vendor access.

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

PowerSchool Data Breach: What Happened and What Families Should Do | Security.org

Apr 30 — via Security

PowerSchool's December 2024 breach — disclosed in greater scope this month — reportedly exposed records of 62 million students and 9.5 million teachers across North America after attackers reused credentials from a subcontractor to access the unMFA-protected PowerSource support portal. The Texas Attorney General has reportedly sued PowerSchool for negligence over absent MFA and encryption, and exfiltrated data included bus-stop and transportation routes — adding a child-safety dimension to FERPA exposure already cascading to thousands of school districts.

Governance signal: Enforce vendor MFA, subcontractor disclosure, and audit rights in K-12 procurement.

Post

2

Ransomware Hit the Company That Runs 80% of Dutch Hospitals - State of Surveillance

Apr 23 — via State of Surveillance

On April 7, ransomware reportedly disabled ChipSoft's HiX EHR platform, which underpins patient records at roughly 70–80% of Dutch hospitals; eleven hospitals disconnected entirely while Z-CERT instructed sector-wide VPN disconnection and traffic-log audits. ChipSoft stated it 'cannot rule out' that patient data was accessed, leaving hospitals dependent on vendor forensics to meet GDPR Article 33/34 deadlines and exposing the latent NIS2 and DORA concentration-risk gap that vendor frameworks rarely treat as a discrete category.

Governance signal: Treat single-vendor concentration as a measurable, board-level resilience risk.

Post

3

Major critical infrastructure supplier reports cyberattack | Cybersecurity Dive

Apr 30 — via Cybersecurity Dive

Itron — a critical-infrastructure supplier serving over 7,700 utility providers across 100 countries — disclosed an April 13 cyberattack via SEC filing, stating it has not observed unauthorized access to customer data. Framed for capital markets rather than for downstream operators, the disclosure reportedly leaves dependent utilities to determine within days whether the incident triggers their own NIS2, DORA, sectoral, and national critical-infrastructure notification obligations without independent forensic visibility.

Governance signal: Vendor SEC disclosures do not satisfy operators' own regulatory clocks.

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

Adobe Data Breach 2026: Mr. Raccoon Leaks 13M Support Tickets | The CyberSec Guru

Apr 09 — via The Cyber Secguru

An Indian BPO support agent for Adobe was reportedly phished and compromised; attackers installed a RAT, escalated to manager credentials, and exfiltrated 13 million support tickets and 15,000 employee files in what the report describes as a single bulk request from one agent account. No rate-limit alert fired, no DLP rule triggered, and the BPO SOC did not flag a support agent behaving like a database administrator — exposing the predictable cost-driven security gap between enterprise standards and outsourced support providers.

Governance signal: Mandate DLP, rate-limits, and aligned SOC alerting for outsourced support vendors.

Post

2

PBSD victim of $3.2 million cybersecurity incident - Pine Bluff Commercial

Apr 30 — via Pbcommercial

An attacker compromised a Pine Bluff School District email account, waited for a legitimate vendor invoice, and injected fraudulent wire-transfer instructions into the existing thread; the finance director processed the $3.2 million payment before contacting the vendor directly surfaced the fraud. The district added dual verbal authorization and removed email-based wire instructions only after the loss, and an FBI nondisclosure order delayed board notification — exposing the gap between vendor risk, finance controls, and incident-disclosure protocols that NIS2 and DORA increasingly treat as a single accountability surface.

Governance signal: Verify every payment-instruction change out-of-band, before transfer, every time.

Post

3

Supply chain attack: Security scanner compromise leads to widespread infostealer and ransomware pivot | ThreatLocker Blog

Apr 21 — via Threatlocker

On February 28, TeamPCP exploited a CI/CD privilege-escalation in the Trivy repository to obtain a personal access token; despite a March 1 remediation, the attackers retained access because rotation was non-atomic — some surviving tokens were used to capture the newly-issued credentials before they could be deployed. The compromise then cascaded into PyPI hijacking of LiteLLM (versions 1.82.7 and 1.82.8) and a partnership with the Vect ransomware group on BreachForums — a chain that atomic credential rotation, build attestations, and SBOM enforcement on critical OSS dependencies would have foreshortened or blocked entirely.

Governance signal: Rotate all related credentials atomically; require SLSA and SBOMs for OSS.

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 — April 2026

Date	Incident	Source	Link
Apr 06	**The Supply Chain Trap: Why Your Vendors Are Your Biggest Security Risk | Giga-Green** *Vendor cybersecurity is routinely treated as a technical problem—a matter of security questionnaires, certifications, and penetration testing.*	*via Giga Green*	Post
Apr 06	**Alleged Contract and Vendor Data of ICE and DHS Leaked** *Summary withheld (insufficient post detail).*	*via Brinz Tech*	Post
Apr 06	**Crunchyroll Hack Exposes Customer Support Data in Vendor Security Incident** *The Crunchyroll incident—in which attackers compromised a single customer support agent's Okta SSO credentials at vendor Telus International to access 8...*	*via CX Today*	Post
	Also covered by: Complex		
Apr 06	**IT Nightmares 002 - RMM Gone Rogue | Guest James Wroten** *When a Remote Monitoring and Management (RMM) platform becomes the attack vector for enterprise-scale ransomware, the failure is structural, not merely...*	*via Channel Pro Net Work*	Post
Apr 06	**Panera's 5.1 Million User Breach: When 'No Hack' Becomes a Ransomware Business Model - Security Boulevard** *The Panera Bread breach—affecting 5.1 million customer records through what Security Boulevard identifies as potential third-party vendor compromise—exposes a s*	*via Security Boulevard*	Post
Apr 06	**Tracking TeamPCP: Investigating Post-Compromise Attacks Seen in the Wild | Wiz Blog** *Summary withheld (insufficient post detail).*	*via Wiz*	Post
Apr 06	**Biggest Data Breaches of 2025: The New Cost of Connectivity - Proven Data** *Summary withheld (insufficient post detail).*	*via Pro Vendata*	Post
Apr 06	**Healthcare Supply Chain Hit as CareCloud Breach** *The CareCloud breach—affecting 45,000+ healthcare providers and exposing millions of patient records—is not primarily a cybersecurity incident.*	*via The Meridiem*	Post
Apr 06	**Your Supply Chain Breach Is Someone Else's Payday** *Summary withheld (insufficient post detail).*	*via Substack*	Post

Apr 06	**Healthcare Software Company Announces Breach of its Electronic Health Record Environment** *When CareCloud, a New Jersey-based electronic health record software provider, announced unauthorized access to one of its six EHR environments, the breach did...*	*via HIPAA Journal*	Post
Apr 06	**Why Third-Party Risk Is the Biggest Gap in Your Clients' Security Posture** *Third-party risk has evolved from a peripheral compliance concern into a material governance liability that directly shapes breach probability, regulatory...*	*via The Hacker News*	Post
Apr 06	**Rethinking Vendor Risk in Healthcare Data Security** *Healthcare organizations have invested billions in perimeter defense, yet third-party vendors account for approximately 80% of stolen protected health...*	*via Seniorexecutive*	Post
Apr 06	**[AKIRA] - Ransomware Victim: Serap - RedPacket Security** *Summary withheld (insufficient post detail).*	*via Red Packet Security*	Post
Apr 06	**Marquis bank data breach exposes 672,000 in ransomware attack | Fox News** *The Marquis ransomware incident—affecting over 672,000 individuals through a Texas-based fintech vendor serving hundreds of banks—represents a structural...*	*via Fox News*	Post
Apr 06	**Corewell Health Vendor Breach Exposes Data of 19,000 Patients** *The Corewell Health incident—where vendor Pinnacle Holdings' November 2024 compromise exposed 19,000 patients' Social Security numbers, financial records, medic*	*via Beyondmachines*	Post
Apr 06	**Banking tech data breach exposes 672K in ransomware attack - CyberGuy** *A ransomware attack against a banking technology vendor has exposed sensitive personal and financial information for over 672,000 individuals.*	*via Cyber Guy*	Post
Apr 06	**[AKIRA] - Ransomware Victim: Swagelok - RedPacket Security** *When a mid-market industrial vendor becomes a ransomware victim, governance implications extend far beyond that organization's perimeter.*	*via Red Packet Security*	Post
Apr 06	**Health data giant CareCloud says hackers accessed patients' medical records | TechCrunch** *CareCloud's confirmed unauthorized access to patient electronic health records—affecting 45,000+ healthcare providers and millions of patients—represents more...*	*via TechCrunch*	Post

Apr 06	**Third-party hack affirmed by Nissan after Everest ransomware assertions | brief | SC Media** *When Everest ransomware operators publicly announced the exfiltration of 910 GB of Nissan customer and dealership data from a third-party vendor, the automaker...*	*via SC World*	Post
Apr 06	**Mercor, a $10 billion AI startup, confirms it was the victim of a major cybersecurity breach | Fortune** *Mercor, a $10 billion AI training-data vendor serving Anthropic, OpenAI, and Meta, suffered a supply-chain attack through the LiteLLM open-source...*	*via Fortune*	Post
Apr 06	**Supply Chain Cyberattacks: How They Work & Spread** *Supply chain cyberattacks represent a governance liability crisis, not merely a technical incident category.*	*via The Cyber Signal*	Post
Apr 06	**Healthcare cyberattack hits TriZetto, 3.4 million affected | Fox News** *The TriZetto breach affecting 3.4 million patient records is not fundamentally a technology failure—it is a governance and contractual accountability failure th*	*via Fox News*	Post
Apr 06	**Cloud-Based EHR Vendor Notifies SEC About Hacking Incident** *When CareCloud, a cloud-based EHR vendor serving over 40,000 healthcare providers across all 50 states, disclosed a March 2026 hacking incident to the SEC, it...*	*via Bank Info Security*	Post
Apr 09	**Five Ways to Build a Security Roadmap with AI — The Last One Changes the Decision** *We asked the same CISO planning question five ways.*	*via*	Post
Apr 09	**NDPC probes Remita, Sterling Bank over alleged data breach - Businessday NG** *The Nigeria Data Protection Commission's simultaneous investigation into Remita Payment Services Ltd.*	*via Businessday*	Post
Apr 09	**Why Third-Party Risk Is Reshaping Cybersecurity In 2026** *Third-party compromise has transitioned from a vendor management concern to a board-level governance and regulatory liability issue.*	*via Cyble*	Post
Apr 09	**HackerOne Gets Hacked: Bug Bounty Giant Falls Victim to Third-Party Breach - State of Surveillance** *When a security platform built on vulnerability identification falls victim to a basic API authentication flaw at a benefits administrator vendor, the implicati*	*via State of Surveillance*	Post
Apr 09	**NYS school data incidents surged in 2025 - Newsday** *New York State school districts reported a 72% surge in data incidents in 2025—from 384 to 662 cases—with one-third (230 incidents) attributed to unauthorized a*	*via News Day*	Post

Apr 09	**Third-party hack affirmed by Nissan after Everest ransomware assertions** *The Nissan incident—in which a third-party vendor compromise led to confirmed data exposure via Everest ransomware—represents a structural breakdown in vendor...*	*via SC World*	Post
Apr 09	**2026 Supply Chain Risk: 5 Critical Reality Checks** *Summary withheld (insufficient post detail).*	*via Cyber Strategyinstitute*	Post
Apr 09	**Meta freezes AI data work after breach puts training secrets at risk** *Summary withheld (insufficient post detail).*	*via The Nextweb*	Post
Apr 09	**Meta Pauses Work With Mercor After Data Breach Puts AI Industry Secrets at Risk | WIRED** *Meta's indefinite pause of work with data contractor Mercor following a breach of proprietary AI training data is not a routine vendor management decision—it...*	*via Wired*	Post
Apr 09	**OpenAI and Anthropic's Data Supplier Was Hacked—Here's What We Know** *Summary withheld (insufficient post detail).*	*via Outlookbusiness*	Post
Apr 09	**Healthcare Supply Chain Hit as CareCloud Breach Exposes Patient Data** *The CareCloud breach—affecting 45,000+ healthcare providers through a single vendor infrastructure—is not primarily a cybersecurity incident.*	*via The Meridiem*	Post
Apr 09	**CareCloud breach exposes millions of patient records** *When a single electronic health record vendor serving 45,000+ healthcare providers experiences a security breach affecting millions of patient records, the...*	*via Tech Buzz*	Post
Apr 09	**Healthcare software firm CareCloud informs SEC of potential patient data leak | The Record from Recorded Future News** *A major healthcare software vendor serving 45,000+ providers disclosed unauthorized access to its electronic health record environment to the SEC following a...*	*via The Record*	Post
Apr 09	**Terry Reilly Health Services Patients' Data Exposed in Vendor Breach - NewsChunks** *The Terry Reilly Health Services breach—in which patient data was exposed through a compromise at third-party vendor TriZetto Provider Solutions—reveals a struc*	*via News Chunks*	Post

Apr 09	**Adobe Data Breach 2026: Mr. Raccoon Leaks 13M Support Tickets | The CyberSec Guru** *The alleged Adobe breach through a compromised Indian Business Process Outsourcing (BPO) vendor handling customer support operations represents a structural...*	*via The Cyber Secguru*	Post
Apr 10	**ISMG Editors: Vendor Breaches Expose Healthcare Risk** *Summary withheld (insufficient post detail).*	*via Bank Info Security*	Post
Apr 10	**Telehealth giant Hims & Hers says its customer support system was hacked | TechCrunch** *Summary withheld (insufficient post detail).*	*via TechCrunch*	Post
Apr 10	**One Vendor Got Hacked and 80 Banks Lost Your Data** *The August 2025 Marquis Software Solutions ransomware incident is not a story about a single vendor failure.*	*via Gblock*	Post
Apr 10	**Ransomware attack on Vivaticket disrupts Louvre and major European museums | Cybernews** *The ransomware attack on Vivaticket—a critical ticketing infrastructure provider serving the Louvre, major European museums, and cultural...*	*via Cyber News*	Post
Apr 10	**The external pressures redefining cybersecurity risk | CSO Online** *Thirty-five percent of data breaches originate in third-party networks, yet most organizations treat vendor risk as a procurement or IT operations issue rather...*	*via CSO Online*	Post
Apr 10	**[DRAGONFORCE] - Ransomware Victim: Innovision Holdings - RedPacket Security** *Summary withheld (insufficient post detail).*	*via Red Packet Security*	Post
Apr 17	**The DocketWise Breach: When Your Legal Tech Vendor Is the Weakest Link | PlatinumIDS Blog** *The DocketWise breach—affecting 116,666 immigration clients through compromised legal technology infrastructure—is not primarily a cybersecurity incident.*	*via Platinumids*	Post
Apr 17	**Zephyr Energy Loses £700k In Cyber Hit That Rerouted Contractor Payment - RedPacket Security** *The £700,000 payment interception at Zephyr Energy plc represents a structural blind spot in how organizations manage third-party cyber risk.*	*via Red Packet Security*	Post
Apr 17	**Zephyr Energy cyber hit rerouted contractor payments?** *Summary withheld (insufficient post detail).*	*via Alltoc*	Post

Apr 17	**Vendor Access Becomes Attack Vector as Rockstar Breach** *Summary withheld (insufficient post detail).*	*via The Meridiem*	Post
Apr 17	**[EVEREST] - Ransomware Victim: K Subsea Group - RedPacket Security** *Summary withheld (insufficient post detail).*	*via Red Packet Security*	Post
Apr 17	**NYS school data incidents rose 72% in 2025, with 44 reported on Long Island** *New York State school districts reported 662 data incidents in 2025—a 72% surge from 384 in 2024.*	*via News Day*	Post
Apr 17	**Zephyr Energy loses £700K to contractor payment fraud • The Register** *Summary withheld (insufficient post detail).*	*via The Register*	Post
Apr 17	**Ralph Lauren hit by supply chain attack | DigitalShield** *The Ralph Lauren incident—compromised through a third-party supplier by the CoinbaseCartel threat group—exposes a structural governance gap that extends across...*	*via Escudodigital*	Post
Apr 17	**Zephyr Energy loses £700K to contractor payment fraud • The Register** *Summary withheld (insufficient post detail).*	*via The Register*	Post
Apr 17	**Hong Kong police arrest suspect over 56,000 patient data leak | Healthcare IT News** *The Hong Kong Hospital Authority breach—involving a 30-year-old contractor employee's unauthorized download of 56,000 patient surgical records—is not a...*	*via Healthcare IT News*	Post
Apr 20	**Vendor Breach Crosses Into Systemic Crisis as Anodot** *The Anodot cloud analytics breach—affecting 12+ enterprise customers simultaneously through a single vendor compromise—represents a critical inflection point in*	*via The Meridiem*	Post
Apr 20	**Security Check-in Quick Hits: Major Bank Regulator Hack Fallout, Hertz Vendor Breach, HHS IT Purge Risks, and Crypto DEX Oracle Exploit Dominate the Last 24 Hours** *Summary withheld (insufficient post detail).*	*via Substack*	Post
Apr 20	**[LYNX] - Ransomware Victim: cwwcontractors[.]com - RedPacket Security** *When a third-party vendor appears on a ransomware group's leak site, organizations face an immediate governance crisis: how to respond to unconfirmed claims...*	*via Red Packet Security*	Post

Apr 20	**MSSPs Caught in the Middle of Iran's Cyber Escalation** *When a managed security service provider (MSSP) is compromised and weaponized as a distribution mechanism for downstream attacks, the entire contractual and...*	*via Msspalert*	Post
Apr 20	**MSP cybersecurity news digest, April 7, 2026** *The April 2026 cybersecurity digest documents a critical structural pattern: major service providers suffering breaches not through direct infrastructure...*	*via Acronis*	Post
Apr 20	**County's latest cyberattack disrupts real estate records again | News | winonapost.com** *Winona County's cyberattack on real estate records—attributed to vendor compromise and severe enough to trigger National Guard mobilization—exposes a...*	*via Winona Post*	Post
Apr 20	**Brockton Hospital Ransomware Attack: Downtime Procedures to Continue for Two Weeks** *When Brockton Hospital in Massachusetts experienced a ransomware incident on April 6 that forced a two-week operational recovery window, the extended downtime...*	*via HIPAA Journal*	Post
Apr 20	**Healthcare IT solutions provider ChipSoft hit by ransomware attack** *The ransomware attack on ChipSoft, a major Dutch healthcare IT vendor providing Electronic Health Record (EHR) systems to multiple hospitals, reveals a...*	*via Bleeping Computer*	Post
Apr 20	**HackerOne slams supplier over delayed breach notice | HackerWorkspace** *When HackerOne—a company whose core business is vulnerability discovery and breach prevention—experienced a data breach through vendor Navia Benefit Solutions,...*	*via Hackerworkspace*	Post
Apr 20	**Breach Risk Is Scored. Survival Risk Is Not.** *Three displacement waves are repricing your vendor ecosystem.*	*via*	Post
Apr 21	**Many Mexican Firms Hit by Supply Chain Cyberattacks: Kaspersky** *Summary withheld (insufficient post detail).*	*via Mexicobusiness*	Post
Apr 21	**Ransomware knocks Dutch healthcare software vendor offline • The Register** *On April 7, 2026, ChipSoft—a Dutch healthcare software vendor serving approximately 80 percent of the country's hospital infrastructure—fell victim to a ransomw*	*via The Register*	Post

Apr 21	**NL: Dutch healthcare software vendor goes dark after ransomware attack - DataBreaches.Net** *When a critical healthcare software vendor is taken offline by ransomware and goes dark operationally, the incident is not contained to that vendor's...*	*via DataBreaches.net*	Post
Apr 21	**ChipSoft Hit by Ransomware: 76% of Dutch Hospitals Rely on This One EPD Vendor | myip.foo** *When a single vendor controls electronic patient record systems across 76% of a nation's hospital network, a ransomware incident ceases to be an isolated...*	*via Myip*	Post
Apr 21	**ProxyCare; Oscar Health; AccentCare Announce Data Breaches** *Healthcare organizations face a structural accountability paradox: they retain full HIPAA regulatory liability for breaches occurring within third-party vendor...*	*via HIPAA Journal*	Post
Apr 21	**MSSPs Are the New Target in Login-Based Attacks – Blackpoint Cyber | news | MSSP Alert** *Summary withheld (insufficient post detail).*	*via Msspalert*	Post
Apr 21	**War Comes to the Channel and MSP Disaster Recovery is Simply Inadequate** *When a managed services provider is compromised, the incident does not remain contained.*	*via Channel Pro Net Work*	Post
Apr 21	**Meta Halts Work With Mercor After Major AI Data Breach** *Summary withheld (insufficient post detail).*	*via Tech Juice*	Post
Apr 21	**Supply chain attack: Security scanner compromise leads to widespread infostealer and ransomware pivot | ThreatLocker Blog** *The compromise of Aqua Security's Trivy scanner—a tool deployed across thousands of organizations to reduce security risk—exposes a structural governance fail*	*via Threatlocker*	Post
Apr 22	**Ransomware knocks Dutch healthcare software vendor offline** *When a single software vendor serves 80 percent of a nation's hospitals, a ransomware attack becomes a systemic healthcare crisis, not an isolated incident.*	*via The Register*	Post
Apr 22	**HackerOne Breach: The Third-Party Risk Problem** *Summary withheld (insufficient post detail).*	*via Frontierzero*	Post
Apr 22	**West Australian Power Company Suffers Data Breach, 900,000 People's Details Exposed | The Epoch Times** *Summary withheld (insufficient post detail).*	*via The Epoch Times*	Post

Apr 22	**CareCloud breach leaves scope questions for providers - TechInformed** *Summary withheld (insufficient post detail).*	*via Tech Informed*	Post
Apr 22	**Police arrest contractor after Hospital Authority data leak affecting 56,000+** *The Hospital Authority breach—involving a systems developer employed by an outsourced maintenance contractor who extracted 56,000+ patient records—exposes a...*	*via Dimsum Daily*	Post
Apr 22	**Mercor Hit With 5 Contractor Lawsuits in a Week Over Data Breach - Business Insider** *When multiple contractors file lawsuits against a single vendor within a seven-day window following a data breach, the underlying issue is rarely the breach...*	*via Business Insider*	Post
Apr 22	**Ransomware Knocks Dutch Healthcare Software Vendor Offline** *On April 7, 2026, a ransomware attack rendered ChipSoft—a Dutch healthcare software vendor serving approximately 80 percent of the country's hospitals—offline.*	*via The Register*	Post
Apr 22	**Healthcare data breach hits system storing patient records** *The CareCloud breach—affecting a system used by over 45,000 healthcare providers and supporting millions of patients—is not primarily a technical incident.*	*via Fox News*	Post
Apr 22	**Healthcare IT Solutions Provider ChipSoft Hit by Ransomware Attack** *When a single healthcare IT vendor's security failure forces multiple hospitals across two countries to take critical systems offline, the incident exposes a...*	*via Bleeping Computer*	Post
Apr 23	**Healthcare IT solutions provider ChipSoft hit by ransomware attack | OpenText Cybersecurity Community** *When a critical healthcare IT vendor sustains a ransomware attack, the incident does not remain contained within that vendor's infrastructure.*	*via Opentext Cyber Security*	Post
Apr 23	**Ransomware Hit the Company That Runs 80% of Dutch Hospitals - State of Surveillance** *On April 7, 2026, ransomware disabled ChipSoft's HiX platform—the electronic health record system managing patient data across 70–80% of Dutch hospitals.*	*via State of Surveillance*	Post
Apr 23	**Dutch hospitals face disruptions after ransomware attack on software provider ChipSoft - NewsBreak** *The ransomware attack on ChipSoft, a core software provider to Dutch hospitals, is not simply an operational disruption.*	*via News Break*	Post

Apr 23	**Dutch healthcare software vendor ChipSoft hit by ransomware attack | brief | SC Media** *Summary withheld (insufficient post detail).*	*via SC World*	Post
Apr 23	**Zephyr Energy hackers swiped £700,000 after redirecting a contractor payment | IT Pro** *When Zephyr Energy's US subsidiary lost £700,000 to a contractor payment redirect, the incident was classified as a cyber intrusion.*	*via It Pro*	Post
Apr 23	**Significant Cyber Incidents | Strategic Technologies Program | CSIS** *The Center for Strategic and International Studies' Significant Cyber Incidents database—a 19-year longitudinal record of major breaches since 2006—exposes a st*	*via Csis*	Post
Apr 23	**Ambulances Diverted from Brockton Hospital While Signature Healthcare Deals with Cyberattack** *Summary withheld (insufficient post detail).*	*via HIPAA Journal*	Post
Apr 23	**Telnyx Python SDK Security Notice: Malicious PyPI Versions Identified (March 2026)** *Summary withheld (insufficient post detail).*	*via Telnyx*	Post
Apr 24	**Supply Chain Attack Strikes Ericsson: Analyzing the Third-Party Vendor Breach | Security Arsenal | Security Arsenal** *Summary withheld (insufficient post detail).*		Post
	Also covered by: Telco Magazine, Bleeping Computer		
Apr 24	**Cetera, Ameriprise Sued Over Alleged Data Breaches** *Summary withheld (insufficient post detail).*	*via Wealthmanagement*	Post
Apr 24	**IT Nightmares 002 – RMM Gone Rogue | Guest James Wroten - MSP Services US** *Remote Monitoring and Management (RMM) platforms occupy a uniquely dangerous position in organizational infrastructure: they operate with administrative...*	*via Mspservices*	Post
Apr 24	**Nissan says stolen data came from third-party vendor after hacking group claims breach | The Record from Recorded Future News** *The Nissan incident—where a third-party vendor's file transfer system became the vector for 910GB of customer, dealership, and loan data exfiltration—reveals a...*	*via The Record*	Post

Apr 24	**Mercor breach claims: What happened with the AI recruiting platform data leak** *The Mercor data breach—involving 4 terabytes of sensitive data stolen by the Lapsus$ group through a compromised open-source library (LiteLLM)—represents a...*		Post
Apr 24	**Stryker Hit by Iran-Linked Hackers in Data-Wiping Attack – Archyde** *Summary withheld (insufficient post detail).*	*via Archyde*	Post
	Also covered by: Krebs on Security, Translate, Forrester, Filmogaz		
Apr 24	**Third-Party Risk Management in Cybersecurity Governance** *Third-party risk management has transitioned from a procurement function into a material governance obligation with direct implications for board liability,...*	*via The Last Tech*	Post
Apr 24	**Dutch healthcare software vendor ChipSoft knocked offline by ransomware attack** *When a single software vendor controls patient record systems across 80 percent of hospitals in an entire nation, that vendor has become critical infrastructure*	*via The Register*	Post
Apr 24	**Mercor Among Many Companies Hit by LiteLLM Breach, Probe Underway** *The LiteLLM breach—which compromised thousands of downstream organizations through malicious versions of a widely-adopted Python package—represents a...*	*via Morocco World News*	Post
Apr 29	**Supply chain risk takes center stage in cyber sovereignty as hidden dependencies, long-tail vendors come into focus - Industrial Cyber**	*via Industrial Cyber*	Post
Apr 29	**Supply chain cyberattacks: Hackers are using small vendors to break into bigger companies | Tech News - News9live** *Summary withheld (insufficient post detail).*	*via News 9Live*	Post
Apr 29	**Critical infrastructure giant Itron says it was hacked | TechCrunch** *When Itron—a critical infrastructure technology provider serving over 110 million utility endpoints across energy, water, and gas sectors—experiences...*	*via TechCrunch*	Post
Apr 29	**r/cybersecurity on Reddit: RansomHouse claims breach of a popular Cybersecurity Vendor, possibly Barracuda Networks** *When a cybersecurity vendor itself becomes a breach victim, the structural implications extend far beyond the vendor's own incident response.*	*via Reddit*	Post

Apr 29	**ConnectWise ScreenConnect, Path Traversal leading to RCE, CVE-2024-1709 (High) - DailyCVE** *Summary withheld (insufficient post detail).*	*via Daily Cve*	Post
Apr 29	**Healthcare Vendor Breach Notification: HIPAA Requirements, Timelines, and Patient Letter Templates** *The HIPAA Breach Notification Rule represents one of the most operationally demanding regulatory frameworks in healthcare vendor management.*	*via Accountablehq*	Post
Apr 29	**Frost Bank hit with class-action lawsuits over breach affecting more than 100K** *The Frost Bank data breach affecting approximately 109,000 customers—attributed to unauthorized access through a compromised third-party vendor—represents a...*	*via Ex Press News*	Post
Apr 29	**Medical Device Maker Medtronic Announces Data Breach** *When a foundational healthcare infrastructure vendor—a medical device manufacturer supplying thousands of organizations globally—experiences network compromise...*	*via HIPAA Journal*	Post
Apr 29	**Weeks after security breach incident involving a third party AI tool, billion-dollar US company reveals another exposure that occurred - The Times of India** *Vercel's disclosure of not one but two separate security incidents—one involving a compromised third-party AI tool (Context.ai) that enabled lateral movement...*	*via Times of India*	Post
Apr 29	**Vercel : Weeks after security breach incident involving a third party AI tool, billion-dollar US company reveals another exposure that occurred | - The Times of India**	*via Times of India*	Post
Apr 30	**AI vendor breach causes trouble for Vercel | Cyber Intelligence Briefing – 24 April 2026**	*via S Rminform*	Post
Apr 30	**Itron reports cybersecurity incident with unauthorized system access** *Summary withheld (insufficient post detail).*	*via Street Insider*	Post
Apr 30	**Kaseya VSA ransomware attack - Wikipedia** *The July 2, 2021 Kaseya VSA ransomware attack—which compromised over 1,000 organizations through a single managed service provider (MSP) platform...*	*via Wikipedia*	Post
Apr 30	**HHS Office for Civil Rights (OCR) Breach Portal** *The HHS Office for Civil Rights Breach Portal is a public repository of healthcare data breaches affecting 500+ individuals.*	*via Hhs*	Post

Apr 30	**The Vercel Breach: OAuth Supply Chain Attack Exposes the Hidden Risk in Platform Environment Variables | Trend Micro (US)** *Summary withheld (insufficient post detail).*		Post
Apr 30	**Poor Risk Analysis Cost 4 Firms $1.7 Million in HIPAA Fines** *Summary withheld (insufficient post detail).*	*via GovInfoSecurity*	Post
Apr 30	**Pickett USA Breach: Engineering Data Exposure Linked to US Utilities** *The January 2026 Pickett USA breach—exposing 139 GB of operational engineering data from three major US utilities—is not primarily a technology incident.*	*via Industrial Cyber*	Post
	Also covered by: The Register		
Apr 30	**Gas-to-Energy contractor history riddled with FBI raids, severed banking ties and shell companies - Kaieteur News**	*via Kaieteur News Online*	Post
Apr 30	**American utility firm Itron discloses breach of internal IT network** *Itron, Inc.—a $2.4 billion utility technology vendor managing 112 million endpoints across electricity, water, and gas networks in 100 countries—disclosed an...*	*via Bleeping Computer*	Post
Apr 30	**Utilities Tech Supplier Itron Discloses Cyber-Attack - Infosecurity Magazine** *Itron, a major global supplier of energy and water management systems, disclosed a cybersecurity breach of its IT systems in an SEC 8-K filing on April 24.*	*via Infosecurity Magazine*	Post
Apr 30	**Major critical infrastructure supplier reports cyberattack | Cybersecurity Dive** *When Itron—a critical infrastructure supplier serving over 7,700 utility providers across 100 countries—disclosed a cyberattack on April 13, 2026, the incident...*	*via Cybersecurity Dive*	Post
Apr 30	**Energy and Water Management Firm Itron Hacked - SecurityWeek** *Summary withheld (insufficient post detail).*	*via SecurityWeek*	Post
Apr 30	**Critical infrastructure giant Itron says it was hacked** *Itron's confirmed cyberattack—affecting a company serving 110+ million utility endpoints across water, gas, and electricity infrastructure globally—represents...*	*via TechCrunch*	Post
Apr 30	**Breach Management: How to Respond to Vendor Data Breach** *Summary withheld (insufficient post detail).*	*via Sbs Cyber*	Post

Apr 30	**Not A Vendor, Still A Breach: Vercel's Third-Party Risk Failure** *Third-party risk management frameworks have a critical architectural flaw: they organize exposure around procurement and contracts rather than access and data...*	*via Forrester*	Post
Apr 30	**New Report Finds One in Two U.S. School Districts Experienced a Cybersecurity Incident in 2025** *When one in two U.S.*	*via PR Newswire*	Post
Apr 30	**[QILIN] - Ransomware Victim: Lifeline PCS - RedPacket Security** *The reported QILIN ransomware incident targeting Lifeline PCS, a US-based telecommunications provider, illustrates a structural governance vulnerability that...*	*via Red Packet Security*	Post
Apr 30	**Threat Advisory: Uptick in Bomgar RMM Exploitation** *Summary withheld (insufficient post detail).*	*via Huntress*	Post
Apr 30	**Inditex Flags Contractor Data Leak, Says Client Records Safe (1)** *Inditex's disclosure of a data breach at a former technology contractor—affecting commercial relations data across multiple enterprise clients—reveals a...*	*via Bloomberg Law*	Post
Apr 30	**Inditex flags contractor data leak, says client records safe - FashionNetwork USA** *A reported data breach originating from a former technology contractor serving Inditex exposes a structural vulnerability in how large retail organizations...*	*via Fashion Net Work*	Post
Apr 30	**Itron IT Breach: Utility Firm Discloses Network Intrusion - TechNadu** *Summary withheld (insufficient post detail).*	*via TechNadu*	Post
Apr 30	**Tax documents for school employees potentially stolen across LA County – San Gabriel Valley Tribune** *A potential security incident involving W2Copy, a third-party vendor managing tax documents for LA County Office of Education (LACOE) and affiliated school...*	*via Sgv Tribune*	Post
Apr 30	**Trump, IRS Ask for Pause in $10 Billion Suit Over Tax Data Leak** *Summary withheld (insufficient post detail).*	*via Bloombergtax*	Post
Apr 30	**Major utilities firm Itron breached as hackers infiltrate energy and water management systems** *The Itron breach—affecting a vendor serving 7,700 utilities across 100 countries—is not primarily a technical incident.*	*via Cyber News*	Post

Apr 30	**RansomHouse Claims Breach of $1B Cybersecurity Vendor: Is it Barracuda? | The CyberSec Guru** *When a cybersecurity vendor becomes the attack surface itself, governance implications extend far beyond the breached organization.*	*via The Cyber Secguru*	Post
Apr 30	**Implantable orthopedic device maker TriMed discloses cyberattack** *TriMed's September 2025 cyberattack—involving an eight-day unauthorized access window and compromise of patient identifiers, medical record numbers, and...*	*via Paubox*	Post
Apr 30	**Zephyr Energy loses £700K to contractor payment fraud** *When Zephyr Energy plc, a UK-listed oil and gas company, lost £700,000 to a contractor payment redirect, the incident was characterized as "highly...*	*via The Register*	Post
Apr 30	**Bogus wire transfer bilks millions from Pine Bluff School District - Arkansas Times** *Summary withheld (insufficient post detail).*	*via Ark Times*	Post
Apr 30	**Major critical infrastructure supplier reports cyberattack | Utility Dive** *Summary withheld (insufficient post detail).*	*via Utilitydive*	Post
Apr 30	**Inditex Flags Contractor Data Leak, Says Client Records Safe - Bloomberg** *Inditex's disclosure of unauthorized access to a contractor's systems—coupled with reassurances that customer data remained protected—reveals a structural...*	*via Bloomberg*	Post
Apr 30	**PBSD victim of $3.2 million cybersecurity incident - Pine Bluff Commercial** *Summary withheld (insufficient post detail).*	*via Pbcommercial*	Post
Apr 30	**Data breach hits Humana customers in Texas, five other states** *Summary withheld (insufficient post detail).*	*via Ex Press News*	Post
Apr 30	**Hamilton City Hall Discloses Sixth Privacy Breach in Three Years – TPR Hamilton | Hamilton's Civic Affairs News Site** *Hamilton City Hall's sixth documented privacy breach in less than three years—this time caused by a third-party vendor portal malfunction exposing volunteer...*	*via The Publicrecord*	Post
Apr 30	**Inditex flags contractor data leak, says client records safe - FashionNetwork** *Summary withheld (insufficient post detail).*	*via Fashion Net Work*	Post

Apr 30	**PowerSchool Data Breach: What Happened and What Families Should Do | Security.org** *The PowerSchool data breach of December 2024—affecting 62 million students and 9.5 million teachers across North America—is not primarily a technology failure.*	*via Security*	Post
Apr 30	**Vendor Access Becomes Attack Vector as Rockstar Breach** *Summary withheld (insufficient post detail).*	*via The Meridiem*	Post
Apr 30	**Supply Chain Cyber Attacks Rise, EU Breach Exposes Weakness - CX Today** *The compromise of Trivy—a widely-deployed open-source security scanner affecting 10,000+ repositories—and the subsequent European Commission cloud breach...*	*via CX Today*	Post
Apr 30	**Healthcare Data Breach 2026: What 4 Breaches Reveal** *The healthcare sector absorbed four major breaches in 30 days during March–April 2026—each exploiting a different attack vector, each affecting tens of...*	*via Zeron*	Post
Apr 30	**[COINBASECARTEL] - Ransomware Victim: McCuaig and associates Engineering - RedPacket Security** *The public disclosure of McCuaig and Associates Engineering as a ransomware victim through threat intelligence platforms—rather than through formal vendor...*	*via Red Packet Security*	Post
Apr 30	**Tax documents for school employees potentially stolen across LA County – Orange County Register** *When a third-party vendor serving thousands of public sector employees unilaterally disables access to sensitive tax documentation and conducts its own...*	*via Ocregister*	Post
Apr 30	**February 2026 Healthcare Data Breach Report** *Healthcare organizations operate under a dangerous assumption: that third-party service providers—billing processors, clinical software vendors, administrative...*	*via HIPAA Journal*	Post
Apr 30	**When Your Legal Tech Vendor Gets Breached: DocketWise Incident Exposes 116,666 Immigration Records and a Profession's Blind Spot** *When DocketWise, a widely deployed immigration case management platform, suffered a breach exposing 116,666 individuals' records—including Social Security...*	*via Complexdiscovery*	Post
Apr 30	**A Qualitative Synthesis of Cyberattack Trends in Managed Service Providers: Analyzing Multi-Tenant Vulnerabilities and Mitigation Strategies** *Managed Service Providers occupy a critical but fundamentally underprotected position in enterprise cyber governance.*	*via Mdpi*	Post

Apr 30	**Breach at cybersecurity company exposes client data and surveillance systems | DigitalShield** *A cybersecurity vendor breach exposing client data, plaintext credentials, and administrative access to 1,858 network devices represents a structural failure...*	*via Escudodigital*	Post
Apr 30	**Cyber Threats Intensify as Nearly 9 in 10 Executives Say Their Companies Lack Adequate Protection - Risk & Insurance : Risk & Insurance**	*via Riskandinsurance*	Post
Apr 30	**AI tool Vendor compromise leads to Vercel Data Breach - Cybersecurity Insiders** *The compromise of Context.ai, an AI development tool, and its subsequent weaponization to breach Vercel's infrastructure represents a structural failure in...*	*via Cyber Security Insider S*	Post
Apr 30	**AI tool Vendor compromise leads to Vercel Data Breach** *The Vercel breach—initiated through compromise of Context.ai, an AI tool vendor—represents a structural shift in how organizations must conceptualize cyber...*	*via Cyber Security Insider S*	Post
Apr 30	**The Vercel Breach: OAuth Supply Chain Attack Exposes the Hidden Risk in Platform Environment Variables**	*via Trendmicro*	Post
Apr 30	**Data breach: Citizens flags limited customer impact after vendor data incident amid ransomware claims - InvestmentNews** *The Citizens Financial Group incident—disclosed in April 2026 following a ransomware gang's claim of access to millions of records—exemplifies a structural...*	*via Investment News*	Post
Apr 30	**Discord-Linked Group Accessed Anthropic's Claude Mythos AI in Vendor Breach** *Summary withheld (insufficient post detail).*	*via Hackread*	Post
Apr 30	**[GENESIS] - Ransomware Victim: K2 Electric, Inc - RedPacket Security** *When a mid-market electrical contractor serving the energy sector appears on a ransomware victim database, the incident is rarely isolated to that vendor...*	*via Red Packet Security*	Post
Apr 30	**Anthropic Mythos Breach: Unauthorized Access Reported | The CyberSec Guru** *Unauthorized access to Anthropic's Mythos—a frontier AI model capable of discovering and exploiting zero-day vulnerabilities across major operating systems and...*	*via The Cyber Secguru*	Post
Apr 30	**Frost Bank, Citizens Bank data leak: Hackers set 6-day deadline for full dump** *The Everest ransomware attack targeting Frost Bank and Citizens Bank, with an explicit six-day extortion deadline, exposes critical structural gaps in how...*	*via Cyber News*	Post

Apr 30	**Supply Chain Attack Hits Vercel: User Data is Being Sold on BreachForums For $2M** *On April 19, 2026, Vercel announced a breach originating not from its own infrastructure, but from a compromised employee at Context AI—a third-party vendor.*	*via Ox*	Post
Apr 30	**Citizens, Frost blame vendor after data breach claim | American Banker** *When a single third-party vendor failure cascades across multiple independent financial institutions simultaneously, it reveals a structural governance problem...*	*via American Banker*	Post
Apr 30	**Citizens Bank customers' personal information compromised in data breach | WPRI.com** *When a financial institution's customers suffer data compromise through a third-party vendor breach, the institution becomes the primary liability...*	*via Wpri*	Post
Apr 30	**Citizens Financial Group: Data breach: Citizens flags limited customer impact after vendor data incident amid ransomware claims** *Summary withheld (insufficient post detail).*	*via Rankiteo*	Post
Apr 30	**UPDATED: Citizens Bank Hit With Two Federal Lawsuits | Go Local Prov** *Federal class action litigation following Citizens Bank's April 2026 ransomware incident reveals a critical structural vulnerability in how financial...*	*via Golocal Pro V*	Post
Apr 30	**Extensive Citizens Financial Group, Frost Bank breaches claimed by Everest ransomware | brief | SC Media** *When Citizens Financial Group and Frost Bank disclosed customer data exposure through a third-party vendor breach—while simultaneously denying "direct system...*	*via SC World*	Post
Apr 30	**Citizens Bank Customers Targeted in Third-Party Data Breach | PYMNTS.com** *When Citizens Bank and Frost Bank customers became targets through vendor compromise—with the Everest ransomware group claiming responsibility and threatening...*	*via Pymnts*	Post
Apr 30	**Tax Documents for School Employees Potentially Stolen Across Los Angeles County - CPA Practice Advisor** *The Los Angeles County Office of Education's reported concern about unauthorized access to W-2 documents stored by vendor W2Copy illustrates a structural...*	*via Cpapracticeadvisor*	Post

CYBERSOL NEWS

Cybersol News

Five Ways to Build a Security Roadmap with AI

April 9, 2026

Cybersol published a methodology piece comparing five AI-assisted approaches to CISO security-roadmap planning. The post documents how the fifth approach — governed execution with GOSTA — restructured initiative sequencing and split a single governance deliverable into two distinct artifacts.

Post

Breach Risk Is Scored. Survival Risk Is Not.

April 20, 2026

Cybersol published a long-form analysis arguing that traditional TPRM scoring captures breach risk but not survival risk under three displacement waves repricing vendor ecosystems. The piece references DORA, GOSTA, and Cybersol's open governance work.

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