CYBERSOL

CYBERSOL B.V.

BN3

Bad News on 3rd Parties

Monthly Intelligence on Third-Party Cyber Liability

July 2026

43 third-party incidents tracked

Courts reject vendor-only liability

Patch velocity as market access

Vendor concentration at scale

Cybersol B.V. | The Hague, Netherlands

cybersol.nl

EXECUTIVE SUMMARY

Key Findings

Total Incidents	Sectors Affected	Geographies
43	4	14+

BN3 is Cybersol's monthly intelligence digest tracking third-party incident coverage published on the Cybersol blog. In July 2026, 43 qualifying incidents were tracked, with healthcare, financial services, and government the most represented sectors. Of these, 15 involved ransomware deployment and 28 involved unauthorized data exposure.

Three themes dominated the month. First, liability moved upstream: a federal court in the Oracle Health litigation reportedly rejected eight health systems' vendor-only liability defense, and UWM faces litigation over a breach at its vendor affecting more than 402,000 individuals. Second, regulators reached for market access rather than fines — FedRAMP's director publicly warned slow-patching vendors that they should not be selling to government, positioning patch velocity as a procurement criterion. Third, vendor concentration produced systemic exposure: a single LMS breach placed reported records of 275 million students under a ransom deadline, and one logistics provider's ransomware incident disrupted food supply across multiple Japanese consumer sectors.

Regulatory posture this month centered on notification conduct and procurement leverage rather than new enforcement frameworks.

The month's incidents repeatedly tested whether breach accountability can be transferred by contract; courts and regulators treated it as remaining with the contracting organization.

Key Takeaway: Remediation accountability cannot be outsourced — courts and procurement regulators are treating breach liability as non-transferable, regardless of vendor contract language.

MONTH AT A GLANCE

July 2026 — By the Numbers

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

QUALIFYING INCIDENTS	INVOLVED RANSOMWARE	DATA EXPOSURE
43	**15**	**28**
unique third-party events	34% of total	65% of total

Top Sectors by Incident Count

Sector	Incidents
Healthcare	16
Financial Services	16
Government	9

Incident Types

Type	Count
Data Exposure	28
Ransomware	15

Vendor Dependency Pattern

Pattern	Count
Software Supply Chain	19
SaaS / Cloud Service	11
Healthcare IT	10

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 — July 2026

This edition covers third-party cyber incidents published on the Cybersol blog during July 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 43 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

Judge rules against Oracle Health breach vendor-only liability defense

Jul 29 — via Paubox

A federal court in the consolidated Oracle Health/Cerner breach litigation reportedly rejected eight health systems' defense that liability for the breach rested with the vendor alone. The ruling signals that data protection accountability to patients cannot be outsourced through contract, regardless of indemnification language.

Governance signal: Remediation accountability: breach liability stays with the data controller

Post

2

After Hugging Face breach, FedRAMP chief tells slow-to-patch vendors to stay out of government

Jul 29 — via Nextgov

Following the Hugging Face breach, FedRAMP's director publicly warned that vendors unable to patch vulnerabilities quickly "shouldn't be selling your software to anyone." The reported remarks position patch velocity as a federal market-access criterion, moving vendor cyber maturity from advisory guidance toward procurement enforcement.

Governance signal: Patch latency: patch velocity emerging as procurement qualification criterion

Post

3

UWM sued over vendor data breach

Jul 14 — via National Mortgage News

Mortgage lender UWM faces litigation after a breach at vendor Mercadien reportedly exposed data of more than 402,000 customers across multiple financial institutions. The suit tests whether liability flows upstream to the primary servicer when vendor data-handling obligations are inadequately documented.

Governance signal: Vendor contract: upstream liability despite third-party data custody

Post

Governance lesson: July's regulatory signals moved past fines. A federal court declined to let eight health systems shift breach liability to their vendor, FedRAMP conditioned federal market access on patch velocity, and UWM was sued over its vendor's breach. Accountability is settling on the contracting organization — regardless of indemnification language.

GREATEST PUBLIC IMPACT

BN3-P: Top 3

Scale. Visibility. Real-world consequences.

1

Canvas Ransom Deadline Hits May 6: What 275M Students and 9,000 Schools Are Facing

Jul 20 — via State of Surveillance

The ShinyHunters extortion of Instructure's Canvas LMS reportedly put records of 275 million students across roughly 9,000 schools under a public ransom deadline. A single learning-management vendor's compromise became a systemic exposure for thousands of institutions with limited contractual leverage over incident response.

Governance signal: Concentration risk: one education vendor, a quarter-billion end users

Post

2

Biometrics, diagnoses, and bank details exposed in major healthcare breach

Jul 30 — via Malwarebytes

NYC Health + Hospitals reported exposure of 1.8 million patient and employee records — including biometrics, diagnoses, government IDs, and bank details — traced to a third-party vendor compromise. The breadth of data types in a single vendor pathway multiplies notification obligations and long-term harm to affected individuals.

Governance signal: Access control scope: vendor pathway aggregated the most sensitive data classes

Post

3

After KFC, cyberattack hits Japanese ice cream giant

Jul 30 — via The Economic Times

A ransomware attack on logistics provider Nichirei reportedly disrupted operations at KFC Japan, Ezaki Glico, Kura Sushi, and dozens of downstream customers, causing product shortages. A specialized logistics vendor outside "essential services" classification functioned as a critical infrastructure node with cross-sector blast radius.

Governance signal: Concentration risk: unclassified logistics node with national blast radius

Post

Governance lesson: July's largest impacts were concentration events — one LMS holding 275 million student records, one vendor holding biometrics and bank details for 1.8 million patients and employees, and one logistics provider whose outage emptied shelves across Japan. Single-vendor dependencies are systemic-resilience exposures, not localized breaches.

MOST PREVENTABLE

BN3-C: Top 3

The gap between knowing and doing.

1

CISA contractor leaked AWS GovCloud keys on GitHub

Jul 14 — via Krebs on Security

According to Krebs on Security, a Nightwing contractor working for CISA exposed privileged AWS GovCloud credentials in a public GitHub repository. Automated secret scanning and vendor credential lifecycle enforcement are established controls; their absence at a cybersecurity agency's contractor illustrates the gap between policy and practice.

Governance signal: Access control scope: no secret scanning on vendor-managed repositories

Post

2

CodeRED emergency notification system breach

Jul 30 — via Town of Goshen (MA)

A ransomware incident at OnSolve's CodeRED platform, reportedly involving clear-text password storage, forced municipalities across the US to rebuild their emergency notification systems. Plaintext credential storage on a public-safety platform represents a baseline control failure that vendor security assessments are designed to catch.

Governance signal: Vendor assessment: clear-text passwords on a public-safety platform

Post

3

Mercor's trust in a fraudulent compliance startup exposed 40,000 people

Jul 30 — via Captain Compliance

Mercor reportedly granted data access to a vendor operating under false compliance credentials, exposing personal data of 40,000 individuals and triggering litigation. Vendor identity and credential verification at onboarding is a one-time control whose absence converted a due diligence gap into direct breach liability.

Governance signal: Vendor assessment: onboarding verification treated as formality, not control

Post

Governance lesson: July's preventable incidents trace to basic controls left unapplied — secret scanning on contractor repositories, hashed credential storage on a public-safety platform, and identity verification at vendor onboarding. The technical solutions exist; the contractual obligation to apply them does not.

COMPLETE INDEX

All Incidents — July 2026

Date	Incident	Source	Link
Jul 14	**Discord Reveals Data Breach Following Third-Party Compromise - Infosecurity Magazine** *Third-party customer support platforms represent a structural blind spot in enterprise cyber governance.*	*via Infosecurity Magazine*	Post
Jul 14	**Huntsville Hospital vendor hit by data breach: What patients need to do now - al.com** *When Cerner, a third-party electronic health record vendor serving multiple healthcare systems, notified clients in August 2025 that an unauthorized party had.*	*via AL.com*	Post
Jul 14	**Hackers target NATO cyber coalition member with data leak threat | Cybernews** *Summary withheld (insufficient post detail).*	*via Cyber News*	Post
	Also covered by: The 420		
Jul 14	**CISA Admin Leaked AWS GovCloud Keys on Github – Krebs on Security** *Summary withheld (insufficient post detail).*	*via Krebs on Security*	Post
	Also covered by: Cyber News, Cybersecurity Dive, Nextgov		
Jul 14	**UWM sued over vendor data breach | National Mortgage News** *Summary withheld (insufficient post detail).*	*via National Mortgage News*	Post
Jul 16	**Xsolis Data Breach Hits 8 Health Systems: Healthcare Vendor Incident Analysis** *The Xsolis data breach represents a critical inflection point in healthcare vendor risk governance.*	*via DistilInfo*	Post
	Also covered by: Kroc News, TechRepublic, Cyber News		
Jul 20	**Nintendo Employee Data Breach via TinyPulse SaaS: WebMD Subsidiary Cyberattack Analysis and Third-Party Risk Insights – Rescana** *The Nintendo breach via TinyPulse—a WebMD-owned employee engagement platform—reveals a critical structural vulnerability in how enterprises manage third-party.*	*via Rescana*	Post
	Also covered by: Cyber Defense Magazine		

Jul 20	**35 GB of Keys to the Kingdom: The Accenture '888' Breach Claim and What It Means for Every Client Downstream | ComplianceHub.Wiki** *Summary withheld (insufficient post detail).*	*via ComplianceHub*	Post
Jul 20	**Canvas Ransom Deadline Hits May 6: What 275M Students and 9,000 Schools Are Facing** *The Instructure Canvas incident represents a critical failure point in educational institution vendor governance.*	*via State of Surveillance*	Post
	Also covered by: Malwarebytes, DataBreaches.net		
Jul 20	**Nearly 17,000 Volvo staff dinged in supplier breach** *When a third-party HR processor experiences a breach affecting nearly 17,000 employees across a major automotive manufacturer, the incident exposes three.*	*via The Register*	Post
Jul 20	**Active Exploitation Alert: ShinyHunters Abuse OAuth and Vendor Integrations to Breach Salesforce and SaaS Environments – Rescana** *Summary withheld (insufficient post detail).*	*via Rescana*	Post
	Also covered by: Salesforce		
Jul 20	**Supply Chain Cyberattack Puts Enterprise Trade Secrets at Risk | PYMNTS.com** *The Luxshare ransomware incident—in which RansomHub claimed access to CAD models, circuit board designs, and engineering documentation from Apple, Nvidia.*	*via PYMNTS*	Post
Jul 20	**Citizens Bank and Frost Bank Customers Targeted in Third-Party Data Breach** *Summary withheld (insufficient post detail).*	*via PYMNTS*	Post
Jul 20	**LastPass customer data exposed in new third-party vendor breach - Android Authority** *Summary withheld (insufficient post detail).*	*via Android Authority*	Post
Jul 20	**Cyberattack against Lidl exposes customer data via IT supplier** *The Lidl cyberattack—in which customer data was compromised through an IT supplier's security failure rather than direct assault on the retailer's.*	*via IT-Branschen*	Post
Jul 21	**Stolen iPhone 18 Pro supplier data leaked in Tata breach - Technobaboy** *Summary withheld (insufficient post detail).*	*via Technobaboy*	Post

	Also covered by: Outlookmoney, Rswebsols, Daily Security Review, Brandspurng, Skeletos, Silicon Report, Financialex Press, Gurufocus, Tapa Apac, Timeline Daily, Androidheadlines, Digitaltrends, Bizz Buzz, The Bridgechronicle, Engadget, 9to5Mac, Economic Times, Staradvertiser, Storyboard18, Yahoo, Americanbazaaronline, Moneycontrol, Cpo Magazine, Whalesbook		
Jul 21	**Vendor breach compromises data of 3 million Texas license customers | www.gat.report** *When a third-party vendor serving the Texas Parks and Wildlife Department (TPWD) suffered a breach exposing personal data of 3.087 million hunting and fishing.*	*via GAT Report*	Post
	Also covered by: Fox34		
Jul 21	**Look back: Global security breach affects some Gage County school districts** *When a global software vendor experiences a security breach affecting multiple school districts simultaneously, the incident exposes a structural governance.*	*via Beatrice Daily Sun*	Post
Jul 29	**OpenLoop Health: What the OpenLoop Breach Reveals About Third-Party Healthcare Data Risk** *Summary withheld (insufficient post detail).*	*via Rankiteo*	Post
Jul 29	**Swiss train maker Stadler refuses Everest $12 million ransomware demand | The Record from Recorded Future News** *Summary withheld (insufficient post detail).*	*via The Record*	Post
	Also covered by: The Traveler, Railway Gazette, Help Net Security, Bleeping Computer		
Jul 29	**Judge rules against Oracle Health breach vendor-only liability defense** *A federal court ruling in the consolidated Oracle Health/Cerner breach litigation has dismantled a foundational assumption in vendor risk management: that.*	*via Paubox*	Post
Jul 29	**After voucher data leak, Missouri treasurer's office pointed** *When a state treasury office experiences a data breach involving thousands of student records and parental contact information, the institutional response.*	*via DDD News*	Post
	Also covered by: Missouriindependent, Sedaliademocrat, Daily Journal Online, Fultonsun, Dexterstatesman, Ksmu		
Jul 29	**Hemmersbach ransomware breach: supplier access is the third-party risk | Breach Wire | Supplier Shield** *The Hemmersbach ransomware breach by Qilin reveals a critical governance blind spot: when an IT services provider is compromised, the stolen credentials do not.*	*via Supplier Shield*	Post
Jul 29	**Hacktivists Claim DHS Breach, Exposing ICE Contracts With Over 6,000 Companies** *Summary withheld (insufficient post detail).*	*via Yahoo News*	Post

	Also covered by: MyPrivacy Blog, Gblock		
Jul 29	**Software provider to more than 2,000 US hospitals says hackers stole employee and customer data | The Record from Recorded Future News** *When a software provider serving 2,000+ US hospitals suffers a breach affecting employee, customer, and business partner data, the exposure cascades across.*	*via The Record*	Post
	Also covered by: TechRepublic, Cyber Security Insider S, Cybersecurity Dive, Computing, Security Magazine		
Jul 29	**Notice of Third Party Incident | Ohio University** *When a critical learning management system vendor experiences a breach, the liability chain extends far beyond the vendor itself.*	*via Ohio University*	Post
Jul 29	**Healthcare giant Abbott probes two cyber incidents amid extortion claims | Malwarebytes** *Abbott Laboratories' concurrent investigation of two cyber incidents—affecting Cancer Diagnostics systems and the LabCentral customer portal—reveals a.*	*via Malwarebytes*	Post
Jul 29	**After Hugging Face breach, FedRAMP chief tells slow-to-patch vendors to stay out of government - Nextgov/FCW** *The Federal Risk and Authorization Management Program (FedRAMP) director's public warning following the Hugging Face breach signals a fundamental restructuring.*	*via Nextgov*	Post
Jul 30	**Deutsche Bank Probes Third-Party Cybersecurity Incident After Unsafe Ransomware Group Claims Breach** *The Deutsche Bank incident—a breach at a third-party marketing platform vendor—illustrates a structural governance vulnerability that regulators and boards.*	*via NeuraCyb Intel*	Post
	Also covered by: Computing		
Jul 30	**CodeRED emergency notification NEW system Registration and Sign In Page - Goshen, MA** *The CodeRED ransomware incident—affecting OnSolve's emergency notification platform deployed across U.S.*	*via Town of Goshen (MA)*	Post
Jul 30	**About 900,000 Origin Energy customers affected by hack as company admits it was warned weeks before public told | Australia news | The Guardian** *Summary withheld (insufficient post detail).*	*via The Guardian*	Post
	Also covered by: Bleeping Computer, Cyber Security News		
Jul 30	**Medical Billing Vendor Hack Affects 1.3M Patients** *Summary withheld (insufficient post detail).*	*via Bank Info Security*	Post

Jul 30	**Ransomware attack at health IT vendor exposes 442,000 patients' data - Becker's Hospital Review | Healthcare News & Analysis** *When Unlimited Technology Systems disclosed a ransomware incident affecting 442,000 patient records in October 2025, the breach did not remain contained within.*	*via Becker's Hospital Review*	Post
Jul 30	**Cyberattack Hits Israeli Military Supplier IMCO, 30 Tb of Data Stolen - Islam Times** *Summary withheld (insufficient post detail).*	*via Islam Times*	Post
Jul 30	**Ernst & Young (EY) Investigates Data Breach Involving Third-Party Support Tickets** *Summary withheld (insufficient post detail).*	*via Security Affairs*	Post
	Also covered by: Shield53		
Jul 30	**Medical equipment supplier's cloud applications breached, leaking patient data to hackers** *Healthcare organizations depend on third-party medical equipment suppliers for critical operational continuity.*	*via HealthExec*	Post
Jul 30	**Biometrics, diagnoses, and bank details exposed in major healthcare breach** *NYC Health + Hospitals' exposure of 1.8 million patient and employee records—rooted in an unnamed third-party vendor compromise—reveals a critical governance.*	*via Malwarebytes*	Post
	Also covered by: TechCrunch		
Jul 30	**After KFC, cyberattack hits Japanese ice cream giant - The Economic Times** *The Nichirei ransomware attack—which disrupted operations across KFC Japan, Ezaki Glico ice cream, Kura Sushi, and dozens of other downstream customers—reveals.*	*via The Economic Times*	Post
	Also covered by: TechRadar, Hindustan Times, Manila Times, Pla Net Today, teiss, Nippon.com, The Record		
Jul 30	**Kudankulam Nuclear Plant Contractor Breach 2026: When a Fourth-Party Data Centre Leaks Critical-Infrastructure Blueprints** *When nearly 19,000 files containing Kudankulam Nuclear Power Plant blueprints and supplier information leaked through a contractor's outsourced data centre in.*	*via ComplianceHub*	Post
	Also covered by: Cyber News, Claims Journal, Indiatoday, Aljazeera		

Jul 30	**Sued, Breached, and Betrayed: How Mercor's Trust in a Fraudulent Compliance Startup Exposed 40,000 People to Hackers - Captain Compliance** *The Mercor incident—in which a fraudulent entity operating under false compliance credentials gained access to sensitive data affecting 40,000.*	*via Captain Compliance*	Post
Jul 30	**Coca-Cola confirms cyberattack as Fairlife operations halted** *Summary withheld (insufficient post detail).*	*via FoodNavigator*	Post
Jul 30	**Cloud Data Leak Exposes Thousands of US Defense Contractor Staff - Infosecurity Magazine** *The exposure of 6,000+ Boeing employees' personal data through digital consultancy IMGE's misconfigured cloud infrastructure represents a structural failure in.*	*via Infosecurity Magazine*	Post
Jul 30	**Major OVHcloud Breach Claim: 1.6M Customers & 5.9M Sites | The CyberSec Guru** *The alleged OVHcloud compromise—affecting 1.6 million customer records and 5.9 million hosted websites—represents a critical inflection point for vendor risk.*	*via The CyberSec Guru*	Post

CYBERSOL NEWS

Cybersol News

BN3 — June 2026: 22 Third-Party Incidents Tracked

July 1, 2026

The June 2026 edition of BN3 — Bad News on 3rd Parties — was published on the Cybersol blog. The edition tracked 22 qualifying third-party cyber incidents from public reporting, with executive summary, BN3-R/P/C selections, and full incident index.

Post

Cybersol B.V. — Security Delta (HSD) Premium Partner

July 2026

Cybersol B.V. continues as a Premium Partner of Security Delta (HSD), the Dutch security cluster in The Hague. The partnership connects Cybersol’s third-party liability research with the wider Dutch security ecosystem.

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