CYBERSOL

CYBERSOL B.V.

BN3

Bad News on 3rd Parties

Monthly Intelligence on Third-Party Cyber Liability

June 2026

22 third-party incidents tracked

Vendor concentration risk

Regulatory enforcement of detection gaps

Preventable access-control failures

Cybersol B.V. | The Hague, Netherlands

cybersol.nl

EXECUTIVE SUMMARY

Key Findings

Total Incidents	Sectors Affected	Geographies
22	4	14+

BN3 is Cybersol's monthly intelligence digest tracking third-party incident coverage published on the Cybersol blog. In June 2026, 22 qualifying third-party incidents were tracked across healthcare, government, financial services, education, and technology supply chains. Of these, 5 involved ransomware deployment and 17 involved unauthorized data exposure.

Three themes dominated the month. First, detection latency emerged as the central governance failure: the ICO's £963,900 penalty against South Staffordshire Water followed a 22-month undetected breach, while the NYC Health + Hospitals compromise affecting 1.8 million people ran undetected for eleven weeks. Second, vendor concentration turned single compromises into multi-victim events — one PeopleGIS cloud misconfiguration exposed data across 80 US municipalities, and a single upstream compromise placed ten law firms on the INC Ransom leak site within 48 hours. Third, liability increasingly followed the data rather than the contract, reflected in the reported exposure of a private-equity owner to PowerSchool's breach and a 630GB leak at Apple and Tesla supplier Tata Electronics.

Regulators reinforced this posture through active enforcement, with the ICO penalty and finalized UK operational-incident and third-party reporting rules signaling that vendor failures now trigger direct accountability. The recurring gap was vendor access governance: credential and token compromise, not novel exploitation, drove the month's largest exposures.

Key Takeaway: Detection latency and vendor access control scope — not attacker sophistication — determined which third-party incidents became regulatory and financial liabilities in June.

MONTH AT A GLANCE

June 2026 — By the Numbers

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

QUALIFYING INCIDENTS	INVOLVED RANSOMWARE	DATA EXPOSURE
22	**5**	**17**
unique third-party events	22% of total	77% of total

Top Sectors by Incident Count

Sector	Incidents
Healthcare	10
Financial Services	7
Government	3

Incident Types

Type	Count
Data Exposure	17
Ransomware	5

Vendor Dependency Pattern

Pattern	Count
Healthcare IT	9
Software Supply Chain	6
SaaS / Cloud Service	5

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 — June 2026

This edition covers third-party cyber incidents published on the Cybersol blog during June 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 22 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

ICO fines South Staffordshire Water nearly £1 million following major cyber-attack

Jun 29 — via Trowers

The UK Information Commissioner's Office issued a £963,900 penalty against South Staffordshire Water, a critical-infrastructure operator serving 1.6 million people, after a breach affecting 633,887 individuals went undetected for 22 months. The ICO reportedly found that only 5% of the IT environment was monitored and no vulnerability scanning was performed during the relevant period, treating detection and remediation failure as the enforceable governance gap.

Governance signal: Detection latency now carries direct regulatory penalty exposure.

Post

2

Unprecedented: Private Equity Firm Potentially on Hook for PowerSchool's Data Breach

Jun 27 — via DataBreaches.net

According to DataBreaches.net, a private-equity acquirer may face direct liability for PowerSchool's breach, in which threat actors used stolen vendor credentials to reach school-district systems, with exfiltration reported in September 2024. The reported exposure of an owner to inherited vendor-risk failures challenges the assumed separation between acquisition due diligence and post-close operational accountability under emerging NIS2 and DORA regimes.

Governance signal: Vendor-risk liability can transfer to acquiring owners.

Post

3

CISA's AWS Credential Leak Highlights Urgent Need for Enhanced Contractor Cybersecurity

Jun 09 — via Samsearch

Reporting by SamSearch describes a credential leak tied to a CISA contractor, in which cloud access keys were exposed through a contractor repository, following KrebsOnSecurity's earlier disclosure. The incident highlights the asymmetry between the standards the agency mandates for contractors and its own credential-management practice, raising notification-obligation and privileged-access-governance questions for federally regulated organizations.

Governance signal: Contractor credential governance must match mandated standards.

Post

Governance lesson: June's regulatory actions treat detection and remediation failure as standalone enforcement triggers. The ICO's £963,900 penalty against South Staffordshire Water for a 22-month undetected breach, the reported prospect of private-equity liability for PowerSchool's breach, and CISA's own contractor credential exposure collectively shift accountability toward pre-incident monitoring and vendor access governance rather than the breach event alone.

GREATEST PUBLIC IMPACT

BN3-P: Top 3

Scale. Visibility. Real-world consequences.

1

Breach exposes data of 3 million Texas hunting and fishing license holders, officials say

Jun 27 — via Cbs News

Texas officials disclosed that a breach at a contracted third-party vendor exposed personal data of approximately 3 million hunting and fishing license holders held by the Texas Parks and Wildlife Department. Reporting indicates the vendor was directed to strengthen access controls only after the breach, pointing to absent pre-incident security baselines in state vendor procurement.

Governance signal: Access controls specified after a breach arrive too late.

Post

2

NYC Health + Hospitals breach reaches 1.8 million

Jun 10 — via Paubox

NYC Health + Hospitals, the largest US public health system, reported a third-party vendor compromise affecting 1.8 million individuals. Attackers reportedly maintained undetected access for eleven weeks, exposing a gap in real-time visibility into third-party system activity and HIPAA notification obligations.

Governance signal: Third-party activity requires continuous, not periodic, monitoring.

Post

3

Tata Electronics, a major tech supplier to Apple and Tesla, confirms data breach

Jun 28 — via TechCrunch

TechCrunch reported that Tata Electronics, a component supplier to Apple and Tesla, confirmed a breach involving 630GB of manufacturing specifications and supplier documentation, with files posted to a hacker forum. The incident created contractual notification and supply-chain-continuity exposure for downstream manufacturers, illustrating limited real-time visibility into tier-one supplier breach events.

Governance signal: Tier-one supplier breaches cascade notification duties upstream.

Post

Governance lesson: June's largest exposures — 3 million Texas license holders, 1.8 million NYC Health + Hospitals patients, and a 630GB leak at Apple and Tesla supplier Tata Electronics — are single-vendor dependency events, not localized breaches. Concentration across state, healthcare, and manufacturing supply chains turns one vendor compromise into population-scale exposure that NIS2 and DORA treat as systemic-resilience risk.

MOST PREVENTABLE

BN3-C: Top 3

The gap between knowing and doing.

1

Over 80 US Municipalities' Sensitive Information Exposed in Vendor Cloud Misconfiguration

Jun 10 — via Wizcase

WizCase reported discovery of 86 publicly accessible Amazon S3 buckets operated by municipal software provider PeopleGIS, exposing sensitive citizen data across more than 80 US municipalities. The exposure stemmed from cloud misconfiguration rather than sophisticated intrusion, reflecting absent contractual clauses governing vendor encryption, access controls, and breach notification.

Governance signal: Cloud misconfiguration is a preventable vendor-governance failure.

Post

2

Klue breach exposed Salesforce CRM data through stolen OAuth tokens

Jun 28 — via CSO Online

CSO Online reported that stolen OAuth tokens at vendor Klue exposed Salesforce CRM data belonging to downstream clients, including security firms Huntress and Recorded Future. The breach spread through unrotated authentication tokens rather than perimeter intrusion, exposing blind spots in how organizations audit third-party token permissions and credential-rotation policies.

Governance signal: Vendor OAuth tokens need scoping, rotation, and monitoring.

Post

3

Your Vendor's Breach Is Your Breach: INC Ransom's Law Firm Cluster

Jun 27 — via Purpleshield Security

Purple Shield Security, citing Halcyon research, reported that ten law firms appeared on the INC Ransom leak site within 48 hours, consistent with a single upstream compromise of a shared vendor platform. The clustering pattern reflects concentration risk: organizations outsourced data custody but retained regulatory and contractual liability without operationalizing it in vendor contracts or incident-response protocols.

Governance signal: Shared-vendor concentration converts one breach into many.

Post

Governance lesson: June's preventable incidents trace to basic controls left unapplied — cloud configuration on PeopleGIS's 86 exposed S3 buckets across 80+ municipalities, OAuth token scoping and rotation at Klue, and vendor concentration limits behind INC Ransom's ten-firm law cluster. The technical solutions exist; the contractual obligation to apply them does not.

COMPLETE INDEX

All Incidents — June 2026

Date	Incident	Source	Link
Jun 09	**Beacon Mutual ransomware attack exposed data of 4,500 current and former RI state employees • Rhode Island Current** *The Beacon Mutual ransomware incident—affecting 4,500 Rhode Island state employees through a third-party service provider—illustrates a structural governance...*	*via Rhodeislandcurrent*	Post
Jun 09	**Critical infrastructure giant Itron says it was hacked** *Summary withheld (insufficient post detail).*	*via TechCrunch*	Post
	Also covered by: TechCrunch, TechCrunch, Fyntralink		
Jun 09	**Army Defense Contractor Leaked 70,000 Files Containing Sensitive Information** *The CMI Management breach represents a critical failure in vendor risk governance at the intersection of contractual accountability and regulatory...*		Post
	Also covered by: Cyber News		
Jun 09	**CISA's AWS Credential Leak Highlights Urgent Need for Enhanced Contractor Cybersecurity | SamSearch** *CISA's AWS credential leak incident exposes a structural vulnerability in how federal agencies—and by extension, their entire contractor ecosystems—manage...*	*via Samsearch*	Post
	Also covered by: Digitalassetredemption		
Jun 09	**Salesforce Security Response: Drift App (Salesloft) Unauthorized Access Incident** *The Salesforce Drift app unauthorized access incident illustrates a critical structural vulnerability in enterprise vendor governance: the absence of...*	*via Salesforce*	Post
Jun 09	**City Says Latest Privacy Breach Was Limited, Measures Taken to Prevent a Repeat – TPR Hamilton | Hamilton's Civic Affairs News Site** *The City of Hamilton's sixth privacy breach in under three years—this one triggered by a vendor configuration vulnerability in eScribe's Board Manager...*	*via The Publicrecord*	Post
Jun 09	**Red Hat hit by npm supply■chain attack - here's how to stay safe | ZDNET** *Summary withheld (insufficient post detail).*		Post

Jun 10	**Over 80 US Municipalities' Sensitive Information, Including** *The exposure of sensitive citizen data across 80+ US municipalities through a single vendor's misconfigured cloud infrastructure represents a structural...*		Post
Jun 10	**Oncology Firm Says Vendor Hack Compromised Patient Data** *The Oncology Institute's disclosure of patient data compromise through a third-party billing software vendor illustrates a persistent governance vulnerability:...*	*via Bank Info Security*	Post
	Also covered by: SC World, Rescana, Rescana, Paubox		
Jun 10	**NYC Health + Hospitals breach reaches 1.8 million** *The NYC Health + Hospitals breach affecting 1.8 million individuals represents a critical failure in vendor risk governance at institutional scale.*	*via Paubox*	Post
	Also covered by: Malwarebytes		
Jun 27	**Unprecedented: Private Equity Firm Potentially on Hook for PowerSchool's Data Breach - DataBreaches.Net** *Summary withheld (insufficient post detail).*		Post
Jun 27	**Your Vendor's Breach Is Your Breach: INC Ransom's Law Firm Cluster** *When ten law firms appear on a ransomware leak site within 48 hours, the incident is not ten separate breaches—it is evidence of a single upstream compromise...*		Post
Jun 27	**Polymarket hit by third-party supplier breach; $3 million in user funds stolen | KuCoin** *Third-party supplier compromise represents one of the highest-impact yet most underestimated vectors in financial services governance.*		Post
Jun 27	**Breach exposes data of 3 million Texas hunting and fishing license holders, officials say - CBS Texas** *The Texas Parks and Wildlife Department breach—affecting 3 million hunting and fishing license holders through a contracted third-party vendor—exposes a...*		Post
	Also covered by: News 4Sanantonio, Analyticsinsight, Gbhackers, Gearjunkie, Yahoo, Kcbd, Spreely		
Jun 27	**LastPass hit by new data breach - 4 steps you should take now | ZDNET** *Summary withheld (insufficient post detail).*	*via ZDNet*	Post
	Also covered by: Tech Buzz		
Jun 28	**April Data Breach May Have Impacted All NC Schools; Student & Staff Data Accessed** *Why This Matters at Board and Regulatory Level*	*via Wral*	Post

	Also covered by: Reddit		
Jun 28	**Citizens/Frost Breach: 3.65M Records via One Vendor** *On April 20, 2026, the Everest ransomware group claimed responsibility for exposing 3.65 million records from Citizens Bank and Frost Bank—neither of which...*	*via Cybelesoft*	Post
	Also covered by: Law360		
Jun 28	**Tata Electronics, a major tech supplier to Apple and Tesla, confirms data breach | TechCrunch** *Summary withheld (insufficient post detail).*	*via TechCrunch*	Post
	Also covered by: Offseq, Security Affairs, Co, Zamin, Info Tech Lead, Livemint, Macobserver, Business Standard, Co, Macrumors, Street Insider, Macrumors, Mac Daily News, Igeeksblog, Telegraphindia, The Record, Reuters, India Times, Kelo, 9to5Mac, Outlookbusiness, Tech Times, Latestly, News 4Hackers, Latestly, Windows News, Insider Etail, The Hindu, Az, Devdiscourse, Business Standard, Macrumors, Times of India, First Post, Indianex Press, Biggo, The Tech Portal		
Jun 28	**Klue breach exposed Salesforce CRM data through stolen OAuth tokens | CSO Online** *Summary withheld (insufficient post detail).*	*via CSO Online*	Post
	Also covered by: Help Net Security, Infosecurity Magazine, SecurityWeek		
Jun 28	**Vendor Breaches Announced by Illinois and Virginia Healthcare Providers** *Summary withheld (insufficient post detail).*	*via HIPAA Journal*	Post
Jun 29	**Healthcare AI platform Xsolis suffers data breach impacting 1.4M individuals | TechTarget** *The Xsolis breach—affecting 1.4 million individuals across multiple healthcare organizations through a single vendor compromise—represents a structural failure...*	*via Tech Target*	Post
	Also covered by: TechRepublic, Nchstats, HealthExec		
Jun 29	**ICO fines South Staffordshire Water nearly £1 million following major cyber-attack | Trowers & Hamlins law firm** *The Information Commissioner's Office enforcement action against South Staffordshire Water—a critical infrastructure operator serving 1.6 million...*	*via Trowers*	Post

CYBERSOL NEWS

Cybersol News

BN3 — May 2026 Edition Published

June 1, 2026

Cybersol published the May 2026 edition of BN3, tracking 54 qualifying third-party cyber incidents from public reporting. The edition included the executive summary, month-at-a-glance statistics, BN3-R/P/C selections, and the full incident index.

Post

Cybersol — Security Delta (HSD) Premium Partner

Ongoing, 2026

Cybersol B.V. continues as a Security Delta (HSD) Premium Partner, anchored in The Hague's cybersecurity ecosystem. The partnership supports Cybersol's work on governance infrastructure for third-party cyber risk and liability through 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