Reporting Window
June 1 to June 30, 2026

Audience
PE Owners, Family Offices, Boards, M&A Teams

Sources
ransomware.live, BlackFog, Recorded Future, CYFIRMA, Bitsight, SEC EDGAR

M&A CYBER THREAT INTELLIGENCE REPORT

EXECUTIVE SUMMARY

June 2026 delivered a concentrated wave of high-consequence attacks targeting the manufacturing sector with particular severity: two of India's largest industrial corporations, Tata Electronics and Bajaj Auto, confirmed ransomware incidents within days of each other, while Foxconn's ongoing Nitrogen ransomware fallout continued to surface downstream customer exposure across Apple, Tesla, Dell, and Nvidia supply chains. Healthcare sustained record breach totals, with **NYC Health and Hospitals confirming 1.8 million individuals affected** including biometric fingerprint data, the largest recorded public healthcare breach of 2026. ServiceNow disclosed a June API vulnerability that exposed internal tickets and employee records across its entire hosted customer base, a single platform failure with tens of thousands of downstream enterprise victims. Ransomware now appears in **48% of all breaches globally** per the 2026 Verizon DBIR, with triple extortion (encrypt, exfiltrate, DDoS) becoming standard operating procedure for top-tier groups. Manufacturing led all sectors at **28.9% of global victims** over the trailing 12 months per Bitsight, with Qilin alone claiming an estimated 1,448 attacks in the same window. For PE and M&A teams, June confirms the thesis: every sector in a typical portfolio is under active, sustained attack.

1.8M	48%	28.9%	5-7x	1,448
NYC Health Breach (Biometrics Stolen)	Breaches Now Include Ransomware	Manufacturing Global Victim Share	True Cost vs. Ransom Demand	Qilin Attacks Trailing 12 Months

DOMINANT THREAT ACTORS

Qilin — **1,448 attacks trailing 12mo**

Maintained dominance as #1 ransomware group globally. Led May with 11 claimed victims per BlackFog. Active across healthcare, manufacturing, and legal sectors in June. Credential theft via phishing remains primary vector. Double extortion standard on all operations.

World Leaks — **Tata Electronics June 10**

Claimed Tata Electronics on June 10, publishing 204,341 files totaling 630.4 GB including Apple and Tesla technical drawings, manufacturing records, employee passports, and proprietary schematics. Emerging group with sophisticated data weaponization tactics.

ShinyHunters — **Kodak claimed June 2026**

Claimed Eastman Kodak in June following the massive April Instructure Canvas breach (275M records). Group operating under merged Scattered LAPSUS$ Hunters banner continues to target high-visibility brands for maximum extortion leverage.

Nitrogen — **Foxconn 8TB fallout continues**

Foxconn North American factories confirmed May 12 attack; June saw continued downstream exposure of Apple, Tesla, Dell, Google, and Nvidia schematics from the 8TB exfiltration. Believed to use code derived from Conti 2 builder with ALPHV ecosystem links.

The Gentlemen — **Top 10 industry spread**

CYFIRMA confirmed The Gentlemen as active in June across IT services (Thailand), and continued its 2026 run as a rapidly scaling RaaS. Dual extortion with advanced evasion and cross-platform ransomware deployment. 182 confirmed Q1 2026 victims.

SafePay — **VPN focus June 2026**

CYFIRMA ranked SafePay in top threat actors for the period ending June 23. Primary vector: VPN weaknesses and credential theft. Double extortion. Particularly active against organizations in targeted sectors with unpatched remote access infrastructure.

SECTOR RISK HEATMAP

SECTOR	THREAT LEVEL	SHARE	DEAL RISK
Manufacturing	CRITICAL	28.9% global	IP theft, OT disruption
Healthcare	CRITICAL	Record breaches	HIPAA, biometric data
Financial Tech	CRITICAL	Systemic risk	Cascading bank exposure
Legal / Accounting	HIGH	Top 3 US sector	Client file exfiltration
Construction	HIGH	Active targeting	Contract and bid data
Education / SaaS	HIGH	Supply chain amp	Platform multiplier risk
Real Estate	ELEVATED	June claims filed	PII, SSN class actions
Technology / IT	ELEVATED	KDDI, ServiceNow	14M records at risk

TRIPLE EXTORTION: THE NEW STANDARD

The 2026 Verizon DBIR confirms ransomware now appears in **48% of all breaches**, up from 44% previously. Nearly four in five incidents combine encryption with simultaneous data theft. Triple extortion adds a third layer: DDoS against public infrastructure, direct regulatory complaints under GDPR or HIPAA to trigger government investigations, and direct outreach to victims' customers and patients. The Gentlemen group contacted patients of breached healthcare providers to inform them their records were for sale. For M&A teams: the incident is no longer contained at the company level. It radiates to customers, regulators, and counterparties simultaneously. **Any target that cannot evidence tested incident response is carrying unpriced triple-extortion liability.**

NOTABLE INCIDENTS | JUNE 1 TO JUNE 30, 2026 | 5Ws + HOW

WHO / WHERE	WHAT	WHEN	WHY TARGETED	HOW (VECTOR)	EST. IMPACT
Tata Electronics (Mfg / Electronics, India)	World Leaks published 204,341 files (630.4 GB): Apple and Tesla technical drawings, manufacturing specs, employee passports, and proprietary operational documents. Over 200,000 alleged company files posted publicly.	Claimed June 10; confirmed June 23, 2026	Apple and Tesla tier-1 supplier. Stolen IP directly impacts two of the world's highest-value companies. Maximum geopolitical and commercial leverage.	World Leaks intrusion techniques: sophisticated data exfiltration with dark web publication. No encryption confirmed. Business operations stated unaffected by Tata.	**CRITICAL: 630 GB of Apple and Tesla IP; downstream exposure to both tech giants; Tata share price impact; Apple investigating**
NYC Health and Hospitals (Public Healthcare, US)	1.8 million individuals affected: SSNs, biometric fingerprints and palm prints, medical records, geolocation data, health insurance details, and financial account credentials all exfiltrated.	Access Nov 25, 2025 to Feb 11, 2026; disclosed March 24; Senate HELP Committee inquiry June 2026	Largest public health system in the US. 45,000 employees. Serves low-income and uninsured patients. Third-party vendor access was the breach vector.	Unnamed third-party vendor compromise. 11 weeks of undetected access. Exfiltration of biometric data suggests broad network access across clinical and HR systems.	**CRITICAL: 1.8M records; biometric data irrecoverable; Senate inquiry; ongoing HIPAA investigation; class action exposure**

WHO / WHERE	WHAT	WHEN	WHY TARGETED	HOW (VECTOR)	EST. IMPACT
Bajaj Auto and BATL (Automotive Mfg, India)	Ransomware attack on Bajaj Auto and its subsidiary Bajaj Auto Technology Ltd. Detected at 8:00 AM IST. Regulatory filing to NSE and CERT-In. Manufacturing operations stated unaffected.	June 23, 2026	Major automotive manufacturer. Connected production environments and complex supply chain. Companion attack to Tata Electronics within same week suggests coordinated India manufacturing campaign.	Unknown threat actor. Rapid containment by internal teams and external experts suggests possible VPN or RDP initial access. CERT-In notified per IT Act 2000.	**HIGH: Regulatory filing required; subsidiary BATL also affected; no confirmed data exfiltration; continued investigation**
ServiceNow (Enterprise SaaS, Global)	Unauthenticated API endpoint flaw exploited across hosted customer instances. Attackers queried internal ServiceNow tables containing tickets, employee records, asset data, and operational documentation. Applied patch June 5.	Malicious activity June 2; bug bounty reports June 3 and 4; patch June 5, 2026	ServiceNow is used by tens of thousands of enterprises globally. Single API flaw exposes entire hosted customer base simultaneously. Maximum supply-chain amplification.	Unauthenticated access flaw in hosted API endpoint. Attackers queried instance tables without authentication. Zero-day style window between June 2 and June 5 patch.	**HIGH: Scope spans entire ServiceNow customer base; employee records and internal tickets at risk; vendor-breach-as-attack-surface pattern**
KDDI Email Platform (Telecom, Japan)	Unauthorized access to email platform serving 6 Japanese ISPs: STNet, KDDI Web Communications, JCOM, Chubu Telecom, Nifty, and Biglobe. Up to 14.22 million email addresses and passwords potentially exposed.	Unauthorized access detected June 17; disclosed June 23, 2026	Single platform serving six ISPs creates cascading exposure. Email credentials enable phishing, account takeover, and lateral movement into enterprise environments of affected users.	Vulnerability in third-party software used in the email system. Classic supply-chain vendor exploitation with amplified downstream impact across six ISP customer bases.	**HIGH: 14.22M email and password pairs; six ISPs; credential stuffing risk for all enterprise users of affected accounts**
Nintendo (Consumer Tech / Gaming, Japan)	ShadowByt3$ claimed 859 MB of stolen data: employee names, email IDs, internal surveys, progress plans, analytics on employee sentiment, content libraries, and reports from 2016 to 2026.	June 2026	Global gaming brand with high visibility. Employee sentiment analytics and internal reports represent significant corporate intelligence and reputational risk.	ShadowByt3$ ransomware group. Attack vector not confirmed. HR and internal survey data suggests access to corporate productivity platforms.	**ELEVATED: Employee PII; internal corporate intelligence; reputational exposure; no confirmed customer data**
Kodak (Manufacturing, US)	ShinyHunters claimed ransomware attack against Eastman Kodak. Scope and data volume under investigation. Attack follows ShinyHunters' prolific April and May 2026 campaign.	June 2026	Legacy manufacturer with IP assets and operational data. ShinyHunters explicitly seeks high-visibility brand targets for extortion leverage.	ShinyHunters credential-based intrusion. Lateral movement to corporate file systems. Consistent with group's established supply-chain and brand-targeting methodology.	**ELEVATED: Investigation ongoing; IP and operational data at risk; ShinyHunters track record suggests data publication if no settlement**
KTR Real Estate Advisors (Real Estate, US)	Anubis ransomware group claimed KTR Real Estate Advisors on June 22. Real estate appraisal and consulting firm. Nature and volume of compromised data under investigation.	June 22, 2026	Real estate appraisal firms hold property valuations, client financials, deal terms, and PII that are highly sensitive in M&A; and investment contexts.	Anubis ransomware. Vector not confirmed. Small professional services firm with likely limited security posture relative to data value.	**ELEVATED: Client financial records; property valuations; deal-sensitive data; identity theft risk for HNW clients**

INTELLIGENCE SPOTLIGHT | TRENDS THAT MOVE DEAL VALUATIONS

① India Manufacturing: Coordinated Campaign, Global Supply Chain Risk

Tata Electronics (June 10) and Bajaj Auto (June 23) were confirmed within 13 days of each other, while Foxconn's May attack continued to surface downstream exposure in June. These three incidents affect tier-1 suppliers to Apple, Tesla, Dell, Google, and Nvidia. The supply-chain risk is not theoretical: Apple was confirmed to be investigating the Tata breach. Manufacturing now accounts for 28.9% of all global ransomware victims per Bitsight, a 12-month high. **Investor implication:** Any portfolio company using Indian or Asia-Pacific contract manufacturers must assess those vendor relationships as part of its own security posture.

② Biometric Data: The Irrecoverable Breach Category

NYC Health and Hospitals' 1.8 million-record breach is the first major US healthcare breach to include biometric fingerprint and palm print data at this scale. The strategic implication is severe: you can freeze a credit card, change a password, and obtain a new SSN, but you cannot change your fingerprints. For PE-backed healthcare and insurtech companies that have deployed biometric authentication (check-in, credentialing, access control), a breach creates permanent, irrecoverable identity exposure for every enrolled individual. **Investor implication:** Healthcare and HR-tech targets using biometric systems require an explicit data classification and biometric-specific security assessment pre-close.

③ ServiceNow API: One Flaw, Every Enterprise Customer

The June 2 to 5 ServiceNow API vulnerability window is a textbook supply-chain amplification event. An unauthenticated flaw in a single hosted endpoint gave attackers access to internal tickets, employee records, and operational documentation across every affected customer instance simultaneously. The three-day window before the patch means every organization using ServiceNow during that period should treat themselves as potentially compromised. **Investor implication:** SaaS platform usage maps should be required diligence deliverables. A target using ServiceNow, Salesforce, or similar platforms must confirm whether they were affected by platform-level vulnerabilities in the diligence window.

④ KDDI: 14.22M Credentials and the Enterprise Phishing Pipeline

The KDDI email platform breach exposed up to 14.22 million email addresses and passwords across six Japanese ISPs. From an M&A perspective, the risk is not the breach itself but what comes after: stolen corporate email credentials from ISP-hosted accounts are sold to access brokers and used for phishing, business email compromise, and lateral movement into enterprise environments. Any portfolio company with Japanese operations whose employees use KDDI-affiliate email services should be treated as credential-compromised. **Investor implication:** Cross-border deals involving Japanese targets require credential hygiene verification, specifically for ISP-hosted email systems.

⑤ Triple Extortion Reaches Consumer Level

The Gentlemen ransomware group's tactic of directly contacting patients at breached healthcare providers to inform them their records are for sale represents a qualitative escalation in extortion methodology. This creates panic independent of the victim organization, generates media coverage the victim cannot control, and forces payment decisions at the C-suite level before incident response is complete. The 2026 Verizon DBIR notes ransomware now appears in 48% of all breaches, with triple extortion spreading from healthcare into finance and legal. **Investor implication:** Portfolio company incident response plans must explicitly address consumer notification and media containment as part of the ransomware playbook.

⑥ Real Estate and Appraisal Firms: Emerging PE Roll-Up Target

KTR Real Estate Advisors (Anubis, June 22) and earlier JRK Property Holdings (The Gentlemen, April) signal a sustained campaign against real estate appraisal, consulting, and investment management firms. These organizations hold property valuations, client financials, deal terms, and HNW individual PII. They appear in PE roll-up strategies as add-on acquisitions but rarely receive cyber diligence scrutiny commensurate with the sensitivity of data they hold. The JRK class action has already been filed. **Investor implication:** Real estate and appraisal add-ons carry full inherited breach liability. Diligence must include a pre-close security assessment regardless of deal size.

DEAL TEAM ACTION FRAMEWORK | WHAT SOPHISTICATED CAPITAL DOES DIFFERENTLY

DEAL STAGE	CYBERSWEEP ACTION	WHAT IT PREVENTS	FINANCIAL BENEFIT
Pre-LOI Screening	QuickSweep: dark web broker check, SEC EDGAR cross-reference, external attack surface scan	Bidding on a company in active ransom negotiation; 8-K non-disclosure liability	Walk-away clarity before capital is at risk; avoids inherited breach
LOI / QofE Stage	DeepSweep: full security posture plus third-party vendor map plus biometric data classification	Hidden cyber debt in EBITDA; SaaS platform exposure (ServiceNow, Salesforce model)	Renegotiate price; structure escrow; right-size R&W; insurance premiums
Pre-Close / Integration	TotalSweep: OT/IT gap, pen test, supply-chain vendor sweep, outside counsel assessment	Post-close breach from manufacturing vendor (Tata/Foxconn model); law firm data exposure	Clean close; no post-close surprise disclosures; lower insurance premiums
Post-Close Portfolio	Continuous monitoring via CyberSweep weekly threat intel brief plus dark web credential alerts	Silent hold-period breach destroying exit valuation; pre-exit disclosure obligations	Protects EBITDA; maintains exit multiple; satisfies LP reporting obligations