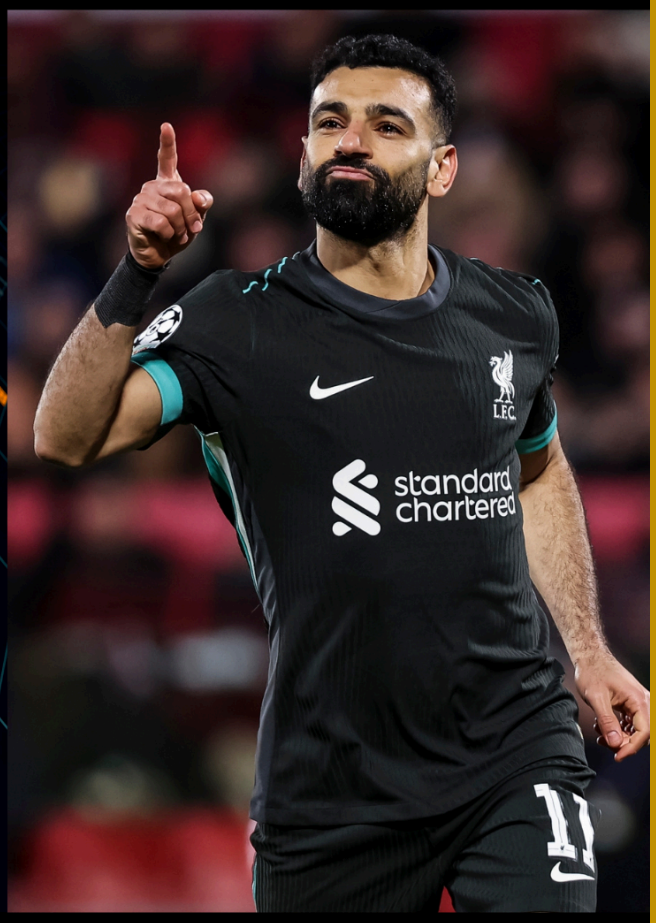
BLOG REPORT

ROI or Ruin: The Critical Data & Cybersecurity KPIs for Sports Private Equity Due Diligence 2.0



TIAKI

Private Equity's New Frontier: Due Diligence in Data, AI, and Cybersecurity for Elite Sports Properties

Private Equity (PE) firms have historically honed their due diligence capabilities with a laser focus on financial metrics, market share, operational efficiencies, and future revenue projections. Their comfort zone lies in dissecting balance sheets, projecting cash flows, and modeling the synergistic effects of strategic acquisitions. This traditional approach has served them well across a myriad of industries. The world of elite sports properties is no exception, having seen significant PE investment in recent years, from football clubs, cricket franchises and basketball teams to F1 franchises and SailGP teams to entire sports leagues.

Traditionally, PE due diligence for sports properties focused almost exclusively on tangible financial metrics and future revenue streams. Key Performance Indicators (KPIs) would revolve around historical ticket sales, broadcast rights agreements, sponsorship valuations, merchandise sales, and projected growth in these areas. Analysis would dissect concession revenues, hospitality package uptake, player salary structures, and stadium operational costs, all culminating in detailed future cash flow projections to determine a return on investment.

A core tenet of private equity, as explored in works such as "Strategic Value Creation" by Rupert Morrison and Jon Andrew[1], is the relentless pursuit of identifying and unlocking latent value within an acquisition. This often involves strategies for operational improvements, market expansion, strategic repositioning, and synergistic bolt-on acquisitions, all designed to generate "breakthrough returns."

While traditional due diligence in private equity has always assessed various forms of risk, it has only recently embraced the critical need to focus on data and cybersecurity risks. But more needs to be done.

The escalating AI-augmented cybercriminal threat landscape, coupled with an expanding attack surface and the aggressive pursuit of data-driven outcomes by leading sports properties, means these risks can no longer be overlooked. The very foundation of future digital revenues and significant value creation is built on data, and the **security of that data is paramount**. The sports industry, in particular, appears to be still playing catch-up in fully integrating these crucial data and cyber risk considerations into their strategic frameworks.

However, the elite sports landscape is undergoing a profound digital transformation. Fan engagement is shifting to digital platforms, athlete performance is meticulously tracked by wearables and analytics, and new revenue streams are emerging from data-driven personalization and digital content.

In this rapidly evolving environment, a critical gap often emerges in the traditional PE due diligence toolkit: a comprehensive assessment of a target property's capabilities and vulnerabilities in data, AI and cybersecurity.

---

[1] Strategic Value Creation: Design and Execute a Strategy for Breakthrough Returns - Rupert Morrison, Jon Andrew - Google Books

This article argues that while not a guaranteed failure, the absence of a robust, resilient data strategy, an intelligent AI roadmap, and an effective cybersecurity posture significantly jeopardizes the anticipated digital monetization of elite sports properties. Moreover, without these critical components, the business is likely to be unacceptably exposed to sophisticated, AI-augmented cybercriminal threats, carrying a high risk of a devastating data breach. Such an incident could not only destroy the acquired company's brand valuation but also erode fan trust, cause strategic suppliers to withdraw, and ultimately prevent investors from achieving a meaningful return on their private equity investment.

Therefore, a thorough data, AI, and cybersecurity assessment is not merely a desirable add-on, but a critical, non-negotiable component of the 2025 private equity due diligence 'tool set' for any sports acquisition. The question for investors is clear: can you afford *not* to assess these risks during due diligence? A pre-deal assessment dramatically improves the odds of success and mitigates potentially catastrophic outcomes.

The Paradigm Shift: Beyond the Balance Sheet

The valuation of an elite sports property today extends far beyond traditional gate receipts, broadcast rights, and merchandise sales. While these remain crucial, the true growth potential increasingly lies in areas heavily reliant on technology: hyper-personalized fan experiences, data-driven athlete performance optimization, global digital content distribution, and the creation of new, interactive revenue streams (e.g., fantasy sports integration, bespoke fan NFTs, advanced betting partnerships).

Private equity firms, in their drive to maximize ROI, must recognize that these future revenue streams and operational efficiencies are not spontaneously generated. They are fundamentally enabled by, and inextricably linked to, sophisticated data infrastructure, intelligent AI applications, and an impregnable cybersecurity defense.

Neglecting these areas is akin to investing in a high-performance race car without checking its engine diagnostics, fuel quality, or braking system – it might look good on paper, but its ability to perform and endure is critically compromised.

Let's delve into each of these three critical domains and outline the key performance indicator (KPI) measurement assessments essential for a holistic PE due diligence.

I. Data: The Foundation of Future Value

In elite sports, **data is the new oil**, encompassing everything from granular fan demographics and engagement patterns to biometric athlete performance data, commercial transaction records, and vast archives of media content. The strategic collection, management, and utilization of this data are paramount for unlocking future value and achieving competitive advantage.

But how do we know if our data is truly healthy and primed for future success? Just as we monitor corporate health with key performance indicators (KPIs), we need similar metrics for our data.

What measures tell you your data is in good shape today and will continue to be reliable and valuable in the next 3, 6, or even 12 months?

Identifying and tracking these data-centric KPIs are crucial for ensuring the sustained health and utility of this invaluable asset.

Significance in Elite Sports:

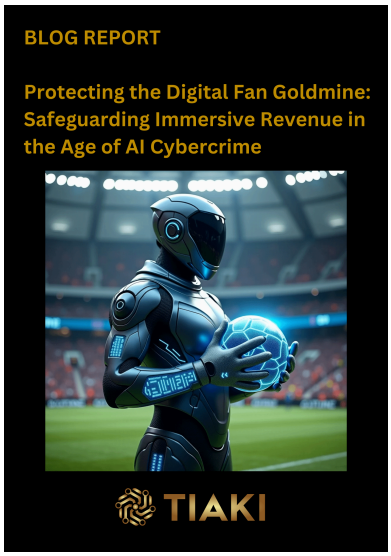
- ★ **Fan Engagement & Personalization:** Understanding fan preferences enables tailored content delivery, personalized marketing, and bespoke product offerings, driving deeper engagement and loyalty.
- ★ **New Revenue Streams:** Data underpins digital monetization strategies, from advanced analytics for betting partnerships to personalized merchandise recommendations and targeted advertising.
- ★ **Athlete Performance:** Real-time and historical data analytics optimize training, prevent injuries, scout talent, and inform strategic decisions on the field.
- ★ **Operational Efficiency:** Data can optimize ticketing strategies, facility management, and logistics, reducing costs and enhancing fan experience.

The Challenge of Social Media Conversion & First-Party Data:

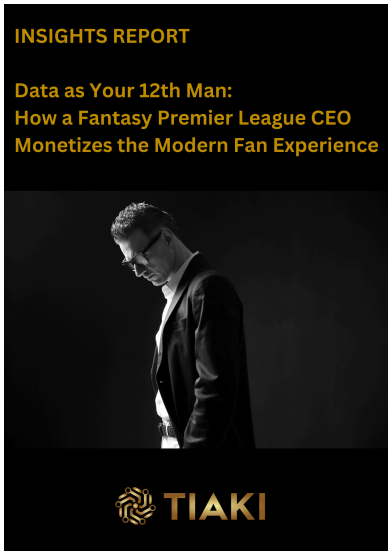
While sports properties boast massive global social media followings, a pervasive struggle exists in converting these passive followers into engaged fans generating digital recurring revenues, largely due to a deficiency in capturing and leveraging quality first-party data at scale.

PE firms must scrutinize the target's current social media engagement strategy not just for reach, but for its effectiveness in driving fans to owned platforms where valuable first-party data can be collected and activated.

Due diligence must identify the root causes of this conversion failure – whether it's inadequate data capture tools, disjointed fan databases, or a lack of personalized engagement strategies – and assess the feasibility of the incoming PE owners to implement the necessary 'data plumbing' and strategic shifts to close this crucial capability gap. True fan value is unlocked by moving direct relationships via first-party data.



In our separate Blog Report, [Protecting the Digital Fan Goldmine: Safeguarding Immersive Revenue in the Age of AI Cybercrime - TIAKI], we highlight 5 potential AI attack vectors and the potential impact on the top 10 European football clubs, and their fan base of 2.3 billion social media followers.



In our separate Blog Report, [Data as Your 12th Man: How a Fantasy Premier League CEO Monetizes the Modern Fan Experience - TIAKI] , we discuss how converting engagement into monetizable data is key to sustained digital growth.

A Premier League club CEO faces significant challenges, including declining traditional revenues, a lack of digital maturity, and severe cybersecurity risks, despite a massive 250 million social media following with less than 0.5% conversion to valuable first-party data.

To overcome the challenges of an evolving digital landscape, a comprehensive digital transformation is planned, focusing on robust **data, AI, and cybersecurity strategies**. The aim is to cultivate first-party fan data and leverage a broader data ecosystem. This ambitious plan, in the article, seeks to convert just 1% of the club's social media followers into recurring digital customers, potentially generating an additional £150 million annually and revolutionizing the club's revenue mix.

While this strategic initiative will undoubtedly appear on the risk register, its profound business impact means it demands direct **CEO ownership and constant oversight**. This isn't just a departmental concern; the success or failure of this transformation, and the mitigation of its associated risks, rests squarely on the CEO's radar. This level of engagement is crucial to safeguard the anticipated revenue growth and the very future of the club's digital endeavors.

The Missing Data Strategy: A Critical Impediment to Digital Growth

A paramount consideration for private equity due diligence is determining whether the sports property has an effective, *deployed* data strategy across the entire organization, or if this critical foundation is missing. The absence of a coherent data strategy materially handicaps and prevents data-driven digital revenue growth. Investors must investigate: Is the sports property crippled by multiple, isolated data silos, or has a strategic consolidation to a unified Customer Data Platform (CDP) taken place? The presence of fragmented data makes it nearly impossible to gain a 360-degree view of the fan, personalize experiences effectively, or identify lucrative monetization opportunities.

Due diligence should therefore include a comprehensive data maturity assessment, benchmarking the property's capabilities against both sports industry best practices and cross-sector leaders. This assessment must identify the specific steps needed to resolve existing data strategy gaps, integrate disparate systems, and build the necessary capabilities to enable future digital revenue streams.

Without a clear path to data consolidation and strategic utilization, the promised ROI from digital transformation will remain elusive.

Risks of Neglect:

- ★ **Failed Digital Monetization:** Without high-quality, integrated data, personalization efforts fall flat, and new digital revenue streams remain theoretical. This is particularly acute for sports properties struggling to convert social media followers into valuable first-party data, often due to a missing data strategy.
- ★ **Missed Opportunities:** Inability to identify emerging trends, optimize performance, or engage fans effectively.
- ★ **Regulatory Penalties:** Poor data governance can lead to hefty fines for non-compliance with privacy regulations (e.g., GDPR, CCPA).
- ★ **Loss of Trust:** Mismanagement or misuse of fan data erodes trust, damaging brand reputation.

10 Data KPI Measurement Assessments for Due Diligence:

1. **Data Governance Maturity (Current Valuation / Risk):**
    - **Assessment:** Evaluate the existence, enforcement, and maturity of data governance policies, data ownership, data stewardship roles, and data privacy frameworks. Look for evidence of a Data Governance Council. Assess how effectively the data strategy is embedded in these governance structures.
    - **KPI:** Data Governance Maturity Score (e.g., 1-5 scale based on documented policies, adherence, and audit trails); Number of defined data owners/stewards per critical data domain; Alignment of data governance with overall data strategy objectives.
2. **Data Quality & Accuracy (Current Valuation / Transformation / Risk):**
    - **Assessment:** Analyze data error rates, completeness, consistency, and freshness across key datasets (e.g., fan profiles, player statistics, ticketing data).
    - **KPI:** Percentage of complete/accurate records for core data entities; Data freshness index (e.g., average latency for critical data updates).
3. **Data Integration & Accessibility (Transformation / Current Valuation):**

- **Assessment:** Map data flows and assess the ease with which data can be accessed and integrated from disparate systems (e.g., CRM, ticketing, performance analytics, merchandise). Critically, identify the extent of data silos versus consolidation efforts.
- **KPI:** Number of siloed data sources; Time required to integrate a new data source; Percentage of data available for analytical consumption across the organization.

4. **Data Volume, Velocity & Growth (Current Valuation / Transformation):**
   - **Assessment:** Understand the scale of data collected, its rate of growth, and the infrastructure's ability to handle increasing volumes (e.g., streaming data, IoT sensors).
   - **KPI:** Total data storage (TB); Data ingestion rate (GB/hour); Projected data growth rate over 3-5 years.
5. **Data Retention & Archiving Policy (Risk / Transformation):**
   - **Assessment:** Review policies for data retention, archival, and deletion to ensure compliance with legal requirements and cost-efficiency.
   - **KPI:** Compliance rate with data retention policies; Cost per GB for data storage and archival.
6. **Data Monetization Pathways (Current Valuation / Transformation):**
   - **Assessment:** Identify existing and potential revenue streams directly linked to data utilization (e.g., personalized advertising, data licensing, fan segmentation for sponsors). Evaluate how the current data strategy (or lack thereof) impacts these pathways.
   - **KPI:** Revenue attributed to data-driven initiatives; Number of identified, unexploited data monetization opportunities; Growth rate of data-driven digital revenue.
7. **Customer Data Platform (CDP) Maturity & First-Party Data Acquisition (Transformation / Current Valuation):**
   - **Assessment:** Evaluate the presence and effectiveness of a centralized platform for creating a unified, 360-degree view of the fan across all touchpoints, with a specific focus on mechanisms to acquire, enrich, and activate first-party data from social media and other owned channels. Assess the level of actual consolidation achieved on the CDP.
   - **KPI:** Percentage of fans with a unified profile on the CDP; Number of marketing/engagement campaigns leveraging CDP insights; First-party data capture rate from digital touchpoints.
8. **Data Talent & Culture (Transformation / Risk):**
   - **Assessment:** Evaluate the availability, skill sets, and retention rates of data scientists, data engineers, and data analysts within the organization. Assess data literacy across non-technical departments, especially concerning the value of first-party data and the adopted data strategy.
   - **KPI:** Data team size and skill gaps; Employee data literacy score; Retention rate of data professionals.
9. **Third-Party Data Sharing Agreements (Risk / Transformation):**
   - **Assessment:** Review all agreements involving third-party data sharing (e.g., sponsors, media partners, betting companies) for clarity, compliance, and mutual value, ensuring adequate safeguards for shared first-party data.
   - **KPI:** Number of non-compliant data sharing agreements; Audit frequency for third-party data handling.
10. **Data Ethics & Privacy Framework (Risk / Current Valuation):**
    - **Assessment:** Examine policies, consent mechanisms, transparency in data collection, and adherence to evolving privacy regulations. Assess the property's reputation regarding data privacy, particularly concerning fan data.
    - **KPI:** Number of privacy complaints; Transparency score (e.g., clarity of privacy policies); Compliance with relevant privacy regulations (e.g., GDPR, CCPA).

—----------

II. Artificial Intelligence: The Performance Multiplier

AI is no longer a futuristic concept but a tangible technology already transforming how elite sports properties operate, compete, and engage with their audience. From optimizing on-field performance to hyper-personalizing fan experiences and predicting market trends, AI is a key differentiator.

Significance in Elite Sports:

- ★ **Athlete Performance Optimization:** AI analyzes vast datasets (biometrics, training logs, match footage) to identify subtle performance trends, predict injury risks, and develop personalized training regimes.
- ★ **Fan Engagement & Personalization:** AI-driven algorithms power recommendation engines for content, merchandise, and experiences, creating deeper, more relevant interactions.
- ★ **Ticketing & Revenue Optimization:** Predictive analytics forecast demand, optimize pricing, and identify opportunities for dynamic pricing and premium packaging.
- ★ **Scouting & Talent Identification:** AI can analyze vast pools of potential athletes, identifying hidden gems and assessing their fit within a team's strategy.
- ★ **Content Generation & Distribution:** AI can assist in generating highlights, translating content, and optimizing distribution channels for maximum reach and engagement.

Risks of Neglect:

- ★ **Competitive Disadvantage:** Falling behind rivals who leverage AI for superior player performance, talent acquisition, and fan engagement.
- ★ **Inefficient Operations:** Missed opportunities for automation and optimization across various business functions.
- ★ **Sub-Optimal Fan Experience:** Generic, untargeted engagement leading to decreased loyalty and reduced digital monetization.
- ★ **AI Bias & Ethical Issues:** Poorly designed or managed AI can perpetuate biases, leading to discriminatory outcomes or reputational damage.

10 AI KPI Measurement Assessments for Due Diligence:

1. **AI Strategy & Roadmap (Transformation / Current Valuation):**
    a. **Assessment:** Evaluate the existence of a clear, documented AI strategy that aligns with overall business objectives and future growth plans.
    b. **KPI:** Presence of an AI roadmap with defined timelines and resource allocation; Number of strategic business units with AI initiatives.
2. **AI Use Case Portfolio (Current Valuation / Transformation):**
    a. **Assessment:** Inventory current and planned AI applications across the organization (e.g., player tracking, fan segmentation, content recommendations, predictive maintenance).
    b. **KPI:** Number of active AI use cases; Percentage of core business processes impacted by AI; ROI for implemented AI solutions.

3. **Data Readiness for AI (Transformation / Risk):**
    a. **Assessment:** Analyze the availability, quality, and accessibility of clean, labeled, and relevant data necessary for training and deploying AI models.
    b. **KPI:** Data preparation time for new AI projects; Percentage of data sources "AI-ready"; Data labeling accuracy rates.
4. **AI Model Performance & ROI (Current Valuation / Transformation):**
    a. **Assessment:** Quantify the measurable impact and ROI of existing AI solutions (e.g., accuracy of predictions, uplift in engagement metrics, cost savings).
    b. **KPI:** Accuracy/precision of key AI models; Attributable revenue increase from AI-driven personalization; Percentage reduction in operational costs due to AI.
5. **AI Talent & Infrastructure (Transformation / Risk):**
    a. **Assessment:** Evaluate the expertise of the in-house AI team (data scientists, ML engineers) and the adequacy of the underlying AI infrastructure (cloud platforms, GPU access, ML Ops tools).
    b. **KPI:** AI team size and skill mix; Cloud AI spend vs. on-premise; Time to deploy a new AI model.
6. **Ethical AI & Bias Mitigation (Risk):**
    a. **Assessment:** Review policies and practices for identifying, measuring, and mitigating bias in AI models. Assess transparency and explainability frameworks for AI decisions.
    b. **KPI:** Existence of an ethical AI framework; Number of bias detection/mitigation techniques employed; Audit frequency for AI model fairness.
7. **AI Integration with Core Systems (Transformation):**
    a. **Assessment:** Determine how seamlessly AI outputs are integrated into operational workflows and decision-making processes across departments.
    b. **KPI:** Number of integrated AI solutions; Latency of AI output integration into business applications.
8. **Innovation Pipeline for AI (Transformation):**
    a. **Assessment:** Evaluate the organization's approach to AI R&D, pilot programs, and partnerships with external AI vendors or academic institutions.
    b. **KPI:** Number of AI prototypes/pilots in development; Budget allocation for AI research and innovation.
9. **Competitive AI Benchmarking (Current Valuation / Transformation):**
    a. **Assessment:** Compare the target property's AI capabilities and applications against those of direct competitors and leading organizations in the broader sports industry.
    b. **KPI:** AI capability gap analysis against top 3 competitors; Ranking in industry AI adoption surveys.
10. **AI Governance & Risk Management (Risk):**
    a. **Assessment:** Review frameworks for managing the lifecycle of AI models, including development, deployment, monitoring, and decommissioning, with a focus on risk mitigation.
    b. **KPI:** AI model inventory and documentation completeness; Frequency of AI model revalidation; Number of AI-related incidents or anomalies.

III. Cybersecurity: The Shield Against Catastrophe

In an increasingly interconnected and digitally driven sports world, cybersecurity is no longer an IT overhead but a strategic imperative. Elite sports properties collect and manage vast amounts of highly sensitive data – from fan personal identifiable information (PII) and financial details to proprietary player health records, strategic playbooks, and valuable broadcast rights. The rise of AI-augmented cybercriminal threats means the risk of a breach is higher than ever, and the consequences could be catastrophic.

The Alarming Reality: Lack of Cybersecurity Resilience

Alarmingly, despite the escalating sophistication of AI-augmented cyber threats, a stark reality is the pervasive lack of robust cybersecurity resilience across most sports properties. This critical vulnerability should be a ***major C-suite and Boardroom concern*** for private equity investors, as it represents an existential threat to brand, revenue, and ultimately, ROI.

The "Agentic Apocalypse"[2] scenario, where AI-powered deepfakes could unleash a "tsunami" on sports ticketing, underscores the rapidly evolving threat landscape. Furthermore, the recent "UK Retail Ransomware Carnage" serves as a stark "Canary in a Coalmine" moment for the sports industry, demonstrating the devastating real-world impact of cyberattacks on business continuity and brand reputation.

In our separate Blog Report, Recent UK Retail Ransomware Carnage is the 'Canary in a Coalmine' Moment for Sport - TIAKI , we highlight the recent ransomware attacks on UK retailers like M&S and Co-op, attributed to groups like Scattered Spider and DragonForce, showcase a significant and escalating cyber threat landscape.

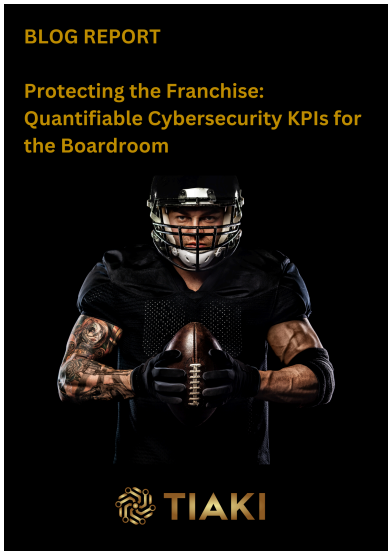
These incidents caused substantial disruption, including online service shutdowns, payment issues, and potential data breaches, leading to considerable financial and reputational damage.

The tactics employed, such as social engineering for credential theft and lateral movement within networks, serve as a stark warning to other sectors, such as sport.

This situation should be viewed as a critical "canary in a coalmine" moment, indicating that the sports industry, with its valuable data and high-profile events, is equally vulnerable to such sophisticated attacks. Proactive and robust cybersecurity measures are now paramount for sports organizations to protect their operations, fan data, and overall integrity against these evolving threats.

---

[2] Agentic Apocalypse: How Google'sAI Checkout Unleashes a 'DeepfakeTsunami' on Sports Ticketing - TIAKI



In our separate Blog Report, [Protecting the Franchise: Quantifiable Cybersecurity KPIs for the Boardroom - TIAKI](), we emphasize the critical need for sports organizations to implement strong cybersecurity governance and utilize Key Performance Indicators (KPIs) to defend against AI-powered cybercrime.

It details how sports teams, as global brands with intricate digital environments, are susceptible to advanced attacks and outlines eight AI-driven attack methods, highlighting the necessity for proactive and data-informed cybersecurity strategies.

The article proposes fifteen cybersecurity KPIs for board and C-suite reviews, such as phishing simulation failure rates, % sanctioned versus % unsanctioned applications, third-party risk management score and account takeover rate with multi-factor authentication (MFA) context, underscoring cybersecurity as a strategic priority to safeguard data, reputation, and fan trust.

Crucially, PE due diligence must determine: Is an effective cybersecurity strategy in place and actively deployed across the organization?

This is not a trivial question. A comprehensive assessment must delve into whether a mature, effective Secure Access Service Edge (SASE) strategy has been defined and rigorously implemented. SASE, by converging network security and wide area networking services, offers a more robust and adaptable security posture, critical for protecting distributed modern sports operations. The absence or immaturity of such a strategy indicates a significant, quantifiable risk. Therefore, a comprehensive cybersecurity maturity assessment, benchmarked against both sports industry best practices and leading cross-sector cybersecurity frameworks, is essential to understand the true risk exposure and the investment required to achieve an acceptable level of resilience.

Significance in Elite Sports:

- ★ **Data Protection:** Safeguarding sensitive fan data, player medical records, financial information, and confidential business strategies from unauthorized access or theft.
- ★ **Operational Resilience:** Preventing disruption to critical systems (ticketing, stadium operations, broadcast infrastructure) from ransomware or denial-of-service attacks.
- ★ **Brand & Reputation:** Maintaining fan trust and a positive brand image by demonstrating robust data protection practices.

- ★ **Regulatory Compliance:** Adhering to stringent data privacy regulations globally, avoiding hefty fines and legal repercussions.
- ★ **Intellectual Property (IP) Protection:** Protecting valuable proprietary algorithms, tactical strategies, and digital content.

Risks of Neglect:

- ★ **Data Breaches:** Loss of sensitive data leading to identity theft, financial fraud, and privacy violations for fans and athletes. This risk is amplified by AI-augmented attack techniques.
- ★ **Ransomware Attacks:** Operational paralysis, significant financial demands, and prolonged disruption to business operations, as seen in recent retail sector incidents which serve as a warning for sports.
- ★ **Reputational Damage:** Severe erosion of brand trust, leading to loss of fans, sponsors, and partners. A major cyber incident can cripple a brand's standing.
- ★ **Regulatory Fines & Legal Action:** Multi-million dollar penalties and lawsuits stemming from non-compliance with data protection laws.
- ★ **Operational Disruption:** Inability to run games, process tickets, or deliver content, leading to direct revenue loss. The impact of such disruptions extends beyond financial losses to core fan experience.
- ★ **Strategic Supplier Exodus:** Partners may cease collaboration due to perceived security risks, impacting revenue streams and competitive positioning.
- ★ **Failure to Achieve ROI:** The aggregate financial and reputational fallout from a major cyber incident can completely negate the anticipated returns on the private equity investment.

10 Cybersecurity KPI Measurement Assessments for Due Diligence:

1. **Cybersecurity Governance & Leadership (Risk / Transformation):**
    a. **Assessment:** Evaluate the presence and authority of a Chief Information Security Officer (CISO), board-level oversight of cyber risk, and clearly defined roles and responsibilities. Assess how regularly and effectively cybersecurity risks are communicated to the C-suite and Board, and whether an effective cybersecurity strategy is actively supported from the top.
    b. **KPI:** CISO reporting structure (e.g., to CEO/Board); Frequency of cyber risk updates to the board; Number of cybersecurity policies and procedures in place; Board's understanding of key cyber risks (quantifiable assessment).
2. **Incident Response Plan (IRP) Maturity (Risk):**
    a. **Assessment:** Review the documentation, testing frequency, and effectiveness of the incident response plan, including communication protocols for stakeholders and regulatory bodies. Special attention should be paid to scenarios involving AI-augmented attacks or deepfake incidents.
    b. **KPI:** Mean Time to Detect (MTTD) incidents; Mean Time to Respond (MTTR) incidents; Frequency of IRP drills/simulations (including tabletop exercises for novel threats); Percentage of identified incidents with a post-mortem review.
3. **Vulnerability Management Program (Risk / Transformation):**
    a. **Assessment:** Examine the rigor of vulnerability scanning, penetration testing, patch management processes, and remediation efforts across all systems and applications, including those handling sensitive fan data and ticketing.
    b. **KPI:** Number of critical/high vulnerabilities; Average time to remediate critical vulnerabilities; Patching compliance rate; Frequency of security assessments on new

AI-powered systems.

4. **Data Encryption & Access Controls (Risk):**
    a. **Assessment:** Verify the implementation of robust encryption for data at rest and in transit, multi-factor authentication (MFA), and least privilege access controls across all fan, player, and financial data.
    b. **KPI:** Percentage of sensitive data encrypted; MFA adoption rate across critical systems; Number of unauthorized access attempts; Regularity of access control audits.
5. **Threat Detection & Monitoring (SIEM/SOC) (Risk):**
    a. **Assessment:** Evaluate the capabilities of the security information and event management (SIEM) system and the presence of a security operations center (SOC), whether in-house or outsourced. Assess their ability to detect AI-augmented attacks and anomalous behaviors, and how these integrate with the overall cybersecurity strategy.
    b. **KPI:** Coverage of logs ingested into SIEM; Number of alerts generated vs. legitimate threats; Time to investigate and classify security alerts; Integration of threat intelligence feeds relevant to sports and retail sectors.
6. **Employee Security Awareness Training (Risk):**
    a. **Assessment:** Review the frequency, comprehensiveness, and effectiveness of cybersecurity training for all employees, including sophisticated phishing simulations and awareness of deepfake threats.
    b. **KPI:** Employee completion rate for security training; Phishing click-through rate; Number of reported suspicious emails; Specific training modules on AI-augmented social engineering.
7. **Third-Party Risk Management (Risk):**
    a. **Assessment:** Scrutinize the processes for assessing and managing the cybersecurity posture of vendors, partners, and suppliers with access to the property's data or systems, particularly those involved in ticketing, broadcasting, and data analytics.
    b. **KPI:** Percentage of high-risk vendors with security assessments; Number of security incidents originating from third parties; Contractual cybersecurity clauses with 3rd parties.
8. **Regulatory Compliance & Certifications (Risk / Current Valuation):**
    a. **Assessment:** Verify adherence to relevant industry security standards (e.g., ISO 27001, NIST Cybersecurity Framework) and data protection regulations (e.g., GDPR, CCPA). Assess the property's proactive stance on emerging privacy legislation and its alignment with the cybersecurity strategy.
    b. **KPI:** Number of compliance audits passed; Number of non-conformities in security audits; Fines/penalties incurred for non-compliance; Certification status eg ISO 27001).
9. **Cyber Insurance Coverage (Risk):**
    a. **Assessment:** Review the adequacy and scope of cyber insurance policies to cover potential costs associated with data breaches, business interruption, and legal liabilities. Ensure coverage reflects the actual risk profile and potential maximum loss scenarios.
    b. **KPI:** Coverage limits vs. estimated maximum loss; Premium cost vs. breach risk reduction; Recency of cyber insurance risk assessment.
10. **Business Continuity & Disaster Recovery (BCDR) (Risk):**
    a. **Assessment:** Evaluate the existence, testing frequency, and effectiveness of plans to restore critical IT systems and business operations in the event of a major cyberattack or disaster, ensuring resilience against disruptive events like ransomware. Assess how these plans integrate with the broader cybersecurity strategy and SASE implementation.
    b. **KPI:** Recovery Time Objective (RTO) for critical systems; Recovery Point Objective (RPO) for critical data; Frequency of BCDR plan testing; Percentage of critical systems included in BCDR.

The 2025 Due Diligence Imperative

The message is clear: for private equity firms targeting elite sports properties, due diligence can no longer be confined to financial statements and market projections. The digital future of sports is intrinsically linked to robust capabilities in data management (especially first-party data acquisition and a deployed data strategy), AI innovation, and, most critically, cybersecurity resilience (including an effective cybersecurity strategy and SASE implementation). These are not merely "IT issues" to be relegated to a technical annex; they are fundamental drivers of future revenue and paramount protectors of existing value.

PE firms must adapt their internal capabilities, perhaps by expanding their due diligence teams to include specialized data scientists, AI ethicists, and cybersecurity experts, or by partnering with external advisory firms with deep expertise in these domains. A superficial checklist approach will no longer suffice. Instead, a deep, analytical dive into the KPIs outlined above is required to truly understand a target's current valuation, the extent of the transformation needed to achieve ROI targets, and the critical risks that could derail the entire investment.

Conclusion

The allure of elite sports properties for private equity investment is undeniable, fueled by passionate fan bases, global appeal, and burgeoning digital opportunities. However, the complexity of these opportunities is matched by the increasing sophistication of the underlying technological infrastructure and the threats it faces.

Data, AI, and cybersecurity are no longer auxiliary considerations; they are the bedrock upon which successful, high-ROI sports investments will be built in 2025 and beyond.

By integrating comprehensive assessments of these critical areas into their due diligence process, private equity firms can go into a deal with their eyes wide open. These findings will be crucial in shaping the key initiatives that must be implemented as part of the value creation plan during the **first 100 days of ownership**. Once that plan is in place, the core data, AI, and cybersecurity initiatives should become the foundation for scaling the business within the first year. Ignoring these elements isn't just a missed opportunity; it's an invitation to significant financial and reputational disaster.

About the Authors:

Jon Andrew
Co-founder
www.arahi.com

Value Creation Planning | Board Pack Reporting | Portfolio Reporting

Jon is the co-founder of Ārahi, a boutique consulting advisory company in the private equity sector in 2021, having spent two decades in Private Equity Value Creation.

Jon started his career with PwC where he worked across the Audit, Training and Transaction Services functions.

He subsequently moved into Private Equity, where he spent more than 13 years in senior roles at Lloyds Development Capital (LDC) and Inflexion, establishing and leading the value creation functions at both firms. His responsibilities included managing LDC's investment in Virgin Racing Formula1 team as the COO.

Jon is a veteran of over 100 value creation programmes and has held a wide variety of roles including CFO, COO, CIO, Executive Chair, and Non-Executive Chair. He currently serves as Chair of a Bridges Fund Management business, Nexgen Services.

Jon is an authority in the Private Equity industry, he leads several flagship courses for the British Venture Capital Association, and is a regular speaker for PEP-Talks, a peer-to-peer network for investment-backed CEOs. Jon is a published author with Strategic Value Creation (2024) which he wrote together with Rupert Morrison.

Jon holds a BSc in Molecular Biology & Biochemistry from the University of Durham and is an ICAEW Chartered Accountant.

David Andrew
Founder & Managing Partner
www.tiaki.ai
david.andrew@tiaki.ai

David is the Founder & Managing Partner at TIAKI, a niche consulting practice helping executive leadership in sport make confident, informed decisions on their risks, investments and business outcomes powered by secure 'data-at-scale'. He collaborates with bold and determined leaders in the sports ecosystem to define their data, AI and cybersecurity strategies to deliver sustainable value.

David's vision for TIAKI is to empower sports franchise CEOs, leadership teams, sports media broadcasters and investors in the global sports industry with strategic advisory frameworks to deliver secure, pioneering digital fan experiences and new ecosystem business models to achieve breakthrough returns.

David has over 20 years of strategy and technology enabled business transformation experience, providing consulting expertise in cloud native technologies, data strategy, digital business enablement and cybersecurity strategy. He is passionate about helping talented leadership teams succeed in securely growing their differentiated business models in the data-driven, digital sports economy.

Based in Stockholm, David previously worked for IBM Consulting, EY, Accenture Strategy and Orange Business. He studied Chemistry at Durham University and holds an MBA from Trinity College, Dublin Business School.