BLOG REPORT

Premier League's Digital VAR: Flagging Revenue, Flawed Data, and Mounting Cyber Risk

TIAKI

Premier League Giants Struggle to Monetize a Billion Social Media Followers

The passionate unwavering support of generations of local fans embedded deep in the local community, the iconic stadiums, the global superstars, the speed and pure physicality of the game – English football, particularly the Premier League, is a phenomenon. Nine of its most prominent clubs – Manchester United, Manchester City, Liverpool, Arsenal, Chelsea, Tottenham, Newcastle, Aston Villa, and West Ham – collectively boast an astonishing estimated one billion+ social media followers.

This immense digital footprint suggests an unparalleled opportunity for engagement and, crucially, monetization. Yet, beneath the surface of fervent online activity, a stark reality exists: these footballing behemoths are significantly underperforming in converting these digital legions into active, repeatable, monetizable fans.

This article delves into the challenging issues and underlying causes of this lack of first-party data, contrasting their struggles with the success of other industries. Furthermore, it highlights a critical, often overlooked, vulnerability: the immature cybersecurity operations and lack of talent that not only hinder digital transformation but also expose these global brands to escalating business risks from increasingly sophisticated, AI-augmented cybercriminals.

Compounding these challenges is the fundamental reality that despite their immense global brand recognition, these Premier League giants often operate with the organizational structures and resource limitations more akin to Small and Medium-sized Enterprises (SMEs) rather than the global corporate titans they appear to be. This ‘small-scale’ factor is a significant underlying cause of their digital conversion failures and immature data and cybersecurity practices.

The Illusion of Influence: Why Followers Don't Equal Fans

The sheer volume of social media followers for Premier League clubs is undeniably impressive. Accounts are flooded with likes, shares, and comments. However, this engagement often remains superficial, existing predominantly within the walled gardens of platforms like Facebook, Instagram, X (formerly Twitter), and TikTok. The critical challenge lies in the clubs' inability to transition these fleeting interactions into valuable, identifiable first-party data.

What is First-Party Data and Why is it Crucial?

First-party data refers to information a company collects directly from its customers or audience. For football clubs, this would include email addresses, phone numbers, purchase history (tickets, merchandise, subscriptions), app usage, website Browse behavior, transactions and engagement with direct club communications. This data is invaluable because it provides a direct, unmediated understanding of individual fan preferences, behaviors, and potential value. It allows for personalized communication, targeted marketing, and the development of tailored products and experiences.

Currently, much of the interaction on social media platforms provides clubs with only aggregated, anonymized data, or general engagement metrics (likes, comments, reach). While useful for broad content strategy, it offers little insight into who precisely these followers are, what motivates their fandom beyond a casual scroll, and how to directly engage them in a way that drives revenue. Sports properties are struggling to keep pace with fragmented consumption habits and convert digital engagement into

direct insight into fan preferences. The issue is highlighted perfectly by a Bundesliga club executive, “We see millions of interactions on our social channels from younger fans, but we have virtually no direct insight into who they are, their preferences, or how to effectively offer them value.”[1]

The Low Conversion Rate: A Digital Desert of Unconverted Potential

While precise, publicly available conversion rates from social media followers to monetizable fans for specific Premier League clubs are scarce, industry experts universally point to alarmingly low figures. Unlike retail or banking, where a social media following often leads to a direct path to purchase or account creation, football fan conversion is significantly more complex and indirect.

Based on aggregated industry insights, the conversion rate of social media followers to actively transacting fans (e.g., season ticket holders, regular merchandise buyers, paid content subscribers) for top Premier League clubs is estimated to be in the **low single-digit percentages, often below 0.5% to 2%**. This means for every 100 social media followers, fewer than two are likely to be generating direct, trackable revenue for the club.

- ★ **Manchester United**, despite its massive 224 million social media followers, would likely see only a fraction of this translate into direct paying customers. Even if a generous 1% convert, that's still only 2.2 million directly monetizable fans from their global digital audience. The remaining 99% represent a vast, unengaged potential.

This dismal figure contrasts sharply with the massive follower counts. This low conversion stems from several factors:

- ★ **Passive Consumption:** Many social media followers are "armchair fans" – they consume content, cheer for their team, but may not have the financial means or geographical proximity to attend games or purchase extensive merchandise. Their engagement is primarily entertainment-driven, not transaction-driven.
- ★ **Lack of Direct Value Exchange:** Clubs often fail to provide compelling reasons for followers to surrender their first-party data. Why should a follower sign up for an email list or download an app if the content they receive isn't significantly more valuable or personalized than what they get on social media?
- ★ **Fragmented Digital Ecosystems:** Clubs often operate disparate digital platforms – an official website, an e-commerce store, a ticketing portal, a club app – with limited integration. This creates a disjointed fan experience and hinders the creation of a unified fan profile to personalise, incentivise and engage.
- ★ **Over-reliance on Sponsorships:** Historically, football clubs have heavily relied on broadcast rights and commercial sponsorships for revenue. This has perhaps de-emphasized the direct-to-consumer (DTC) monetization of their fan bases, leading to a slower adoption of sophisticated data strategies seen in other industries. As Deloitte's Football Money League reports, commercial revenue (largely sponsorship-driven) and broadcast revenue remain the largest sources for top clubs.[2]

The Elusive Customer Lifetime Value (CLV)

Customer Lifetime Value (CLV) is a crucial metric that estimates the total revenue a business can reasonably expect from a[1] customer throughout their relationship. For Premier League clubs, calculating

[1] The Gen Z and Alpha Fan Monetization Paradox in Global Sports - TIAKI
[2] Deloitte Football Money League 2025

an average CLV per fan is challenging due to the lack of comprehensive first-party data. However, industry estimates for a truly engaged, monetizable fan (e.g., a season ticket holder, regular merchandise buyer) can range significantly.

Based on general sports industry benchmarks, a highly loyal, season ticket-holding fan could have a CLV of **€5,000 - €15,000+ over a 10-year period**, factoring in tickets, merchandise, F&B at games, and potentially premium content subscriptions.

However, for the vast majority of those billion social media followers, the CLV is likely close to **zero**. They are not spending money directly with the club. This highlights the critical gap between perceived influence and actual revenue generation. The "average CLV per fan" across the entire social media following would be diluted to an incredibly low figure, as it would include millions of individuals who contribute nothing directly to the club's bottom line. The challenge, therefore, is not just about increasing the CLV of existing paying fans, but about identifying and nurturing the monetizable segment within the broader social media audience.

Horizm's "Digital Value of Fans 2024" report indicates that the "value per fan" for top leagues like the Premier League can be surprisingly low when averaged across all followers, suggesting a wide disparity between passive followers and active consumers.[3]

Value Per Fan: North America versus Europe

Beyond sheer size and total value, the "Digital Value of Fans 2024" report highlights the critical metric of "Value per Fan." This measure reveals which leagues are most efficient at extracting digital value from each of their followers, offering a deeper insight into their content strategies and audience engagement.

The report clearly demonstrates that American leagues are superior in generating value per fan:

- ★ 5 times more efficient compared to aggregated European football leagues
- ★ 3 times more efficient compared to the Premier League.

This is primarily driven by the geographic concentration of their followers in the United States, where Cost Per Mille (CPM) rates for advertising are generally higher.

North America Value per Fan for 2024 season:

- ★ The NFL leads significantly with €1.95 per fan.
- ★ The NHL follows closely at €1.90 per fan.
- ★ MLB comes in strong at €1.73 per fan.

These figures are remarkably higher than those of major European football leagues.

[3] Digital Value of Fans 2024 - Horizm

European Giants Lag in Per-Fan Value:

Despite their massive global audiences, leagues like the Premier League and LaLiga show surprisingly lower value per fan:

- ★ Premier League: €0.57 per fan
- ★ LaLiga: €0.34 per fan
- ★ Bundesliga: €0.36 per fan
- ★ Ligue 1: €0.35 per fan
- ★ Serie A: €0.32 per fan

This wide disparity suggests that while these football leagues have incredible reach, there might be significant untapped potential in their monetization strategies for their broader follower base. The report highlights a gap between passive followers and active consumers, underscoring the need for more targeted engagement and content strategies to boost this metric.

A Tale of Two Strategies: Football vs. Other Industries

The stark contrast between Premier League clubs' digital monetization efforts and those of other consumer-facing industries is glaring. Retail, travel, entertainment (e.g., streaming services, gaming), and banking have aggressively embraced first-party data strategies, demonstrating significantly higher conversion rates and robust CLV models.

Benchmarking Conversion and CLV:

Industry Sector	Social Media Follower to Paying Customer Conversion Rate	Average Customer Lifetime Value (CLV) (Indicative)	How Data is Monetized
Premier League Football Clubs	**0.5% - 2% (estimated)**	**€0 - €15,000+ (highly variable, high-value fans are few)**	Sponsorships, Broadcasting, Ticket Sales, Merchandise (often via third-parties)
Retail (E-commerce)	**2% - 5% (website visitors to buyers)**	**€100 - €1,000+ (driven by repeat purchases, loyalty)**	Personalized recommendations, targeted ads, loyalty programs, subscription boxes
Travel (Airlines/Hotels)	**5% - 15% (website visitors to bookings)**	**€500 - €5,000+ (repeat travel, loyalty tiers)**	Personalized offers, loyalty programs, ancillary services,

			upgrades
Entertainment (Streaming)	**10% - 30%+ (trial to paid subscription)**	**€120 - €600+ per year (recurring subscriptions, add-ons)**	Subscription fees, personalized content, targeted ads, merchandise, events
Banking/Financial Services	**5% - 10%+ (lead to account opening/product uptake)**	**€500 - €5,000+ per year (fees, interest, cross-selling)**	Personalized financial products, targeted offers, advisory services, cross-selling

Why are Football Clubs Failing So Badly?

The reasons for this disparity are multifaceted and deeply rooted in the historical evolution and business models of football clubs:

1. **Legacy Business Models & Complacency:** For decades, football clubs' primary revenue streams have been matchday income (tickets, hospitality), broadcast rights, and commercial sponsorships. These traditional pillars, especially lucrative broadcast deals, have perhaps fostered a degree of complacency regarding the urgent need for direct fan monetization. As Deloitte's 2025 Football Money League shows[4], broadcast and commercial revenues still dominate. While Real Madrid's new stadium has driven significant matchday and commercial uplift, it highlights the importance of physical assets rather than purely digital engagement.

2. **Lack of a Unified Fan ID & Data Silos:** Many clubs lack a single, comprehensive "fan ID" system that aggregates all interactions a fan has with the club – from buying a ticket to visiting the website, engaging on social media, or buying merchandise. Data often resides in separate, incompatible systems (ticketing CRM, merchandise e-commerce, app analytics), making it impossible to build a holistic 360-degree view of the fan. Publicis Sapient's partnership with Manchester City to strengthen their "digital ecosystem" and leverage data capabilities is a recognition of this very problem. ADvendio also highlights the need for 360-degree solutions like Salesforce to manage and monetize fan data.

3. **Content Strategy Misalignment:** Clubs often view social media as a broadcasting channel for match highlights, news, and promotional material rather than a two-way engagement platform designed to capture data and foster deeper relationships. While engagement rates on platforms like Instagram are higher, this doesn't automatically translate to direct revenue. Greenfly emphasizes leveraging short-form content for fan engagement and sponsor activations, but the leap to first-party data collection remains a hurdle.

4. **Limited Direct-to-Consumer (DTC) Offerings:** Beyond tickets and basic merchandise, many clubs have been slow to develop compelling DTC digital products or services that warrant data exchange.

[4] Deloitte Football Money League 2025

This could include premium content (exclusive behind-the-scenes access, tactical analysis), personalized digital experiences, or innovative fan loyalty programs. While some clubs are experimenting with apps and digital content, they often struggle to differentiate from free social media content.

5. **Perceived Value vs. Actual Value for Fans:** Fans are increasingly savvy about their data. They won't willingly provide it unless there's a clear, tangible benefit. Clubs often fail to articulate this value proposition. "Sign up for our newsletter" is no longer enough; fans expect personalized content, exclusive access, or unique experiences in exchange for their information. There is a lack of clear value propositions for highly engaged fans and a need to differentiate benefits for members versus non-members.

6. **Measurement and ROI:** Demonstrating the immediate return on investment (ROI) for significant data infrastructure and personalization efforts can be challenging. This can hinder investment, as a CFO of a European football club admitted: "We know we need to invest in our data infrastructure to truly understand and monetize our younger fans, but demonstrating the immediate ROI to justify that significant upfront cost is a challenge."[5]

The Cybersecurity Blind Spot: A Looming Digital Disaster

Beyond the challenges of data capture and monetization, Premier League clubs face a significant, often overlooked, threat: **immature cybersecurity operations and a critical lack of cybersecurity talent.** This vulnerability is not merely an IT problem; it directly hinders their ability to deliver best-practice digital offerings and dramatically increases business risks, especially as AI-augmented cybercriminals increasingly target the global sports industry.

The Underbelly of Digital Transformation:

While top clubs invest heavily in high-profile digital platforms and flashy fan apps, the foundational security infrastructure often lags and become a lower priority ‘after thought’:

- ★ **Lack of Dedicated Cyber Talent:** Unlike banks or major e-commerce retailers, sports organizations have historically viewed cybersecurity as a secondary concern, often subsumed under general IT. This leads to a severe deficit in dedicated, experienced cybersecurity professionals (CISOs, security analysts, incident responders) who possess the specialized skills to defend complex digital ecosystems.
    - The GOV.UK Cyber Security Breaches Survey 2025 indicates that only 27% of businesses in 2025 have a board member with responsibility for cybersecurity, a decline since 2021, suggesting a continued lack of high-level prioritization. This paints a worrying picture for organizations across sectors, including sports.
- ★ **Fragmented Security Posture:** Just as fan data is siloed, so too are security efforts. Different departments or third-party vendors might manage security for ticketing, merchandise, club apps, and social media, leading to inconsistencies, vulnerabilities, and a lack of a unified security strategy.
- ★ **Inadequate Investment:** Cybersecurity is often seen as a cost center rather than a critical enabler of the business. This results in underfunded security budgets, outdated technologies, and insufficient training for staff.
- ★ **Reliance on Basic Controls:** Many clubs rely on fundamental cybersecurity measures (firewalls, antivirus) but lack advanced threat detection, incident response capabilities, and continuous

[5] The Gen Z and Alpha Fan Monetization Paradox in Global Sports - TIAKI

monitoring, leaving them exposed to sophisticated attacks.

How This Hinders Digital Offerings and Increases Business Risks:

1. **Erosion of Trust and Fan Data Breaches:** Fans will not willingly provide first-party data – email addresses, payment information, personal preferences – if they perceive that the club cannot adequately protect it. A major data breach, exposing sensitive fan information, could lead to a catastrophic loss of trust, reputational damage, significant fines (e.g., under GDPR), and a mass exodus from digital platforms. This directly impacts conversion rates and CLV, as fans become hesitant to engage directly.

2. **Disruption of Digital Services:** Cyberattacks (e.g., DDoS attacks, ransomware) can cripple ticketing systems, official websites, and club apps, preventing fans from buying tickets, accessing content, or engaging with the club. This directly impacts revenue streams and fan experience, leading to frustration and lost opportunities. Imagine a major match day where fans cannot access their digital tickets due to a ransomware attack.

3. **Compromise of Sensitive Club Data:** Beyond fan data, clubs hold vast amounts of sensitive business data: player contracts, financial records, scouting reports, highly confidential player medical data, tactical plans, and intellectual property. A breach of this data could lead to competitive disadvantages, financial losses, major disruption to betting markets and even blackmail.

4. **AI-Augmented Cybercrime: A Growing Threat:** The rise of AI is dramatically escalating the capabilities of cybercriminals.
    - **Automated Attacks:** AI can automate phishing campaigns, malware generation, and vulnerability scanning at an unprecedented scale and speed, making it harder for human defenders to keep up.
    - **Advanced Social Engineering:** AI can craft highly personalized and convincing phishing emails, voice deepfakes, and even video deepfakes, making it incredibly difficult for individuals, including club staff and players, to detect scams.
    - **Sophisticated Malware:** AI can generate polymorphic malware that constantly changes its signature, evading traditional antivirus software.
    - **Increased Targeting of High-Profile Entities:** Global sports organizations, with their vast fan bases, high-value assets, and public profiles, are increasingly attractive targets for state-sponsored actors, organized crime, and hacktivists. The perceived wealth and high-stakes nature of sports make them prime targets for ransomware and extortion.
    - **Exploiting Supply Chain Vulnerabilities:** Clubs rely on a complex ecosystem of third-party vendors for ticketing, merchandise, data analytics, and broadcasting. A weak cybersecurity posture in any of these partners can create a critical vulnerability that cybercriminals can exploit to gain access to the club's systems.

The impact of a cyberattack on a Premier League club goes far beyond financial loss; it can severely damage brand reputation, erode fan loyalty, and disrupt core operations, ultimately hindering their ability to monetize their global fan base effectively.

The SME Paradox: Global Brand, Local Operations

This brings us to a crucial, often overlooked, factor: the **organizational scale of these Premier League clubs**. While they boast global brand recognition, massive social media followings, and multi-million or even billion-pound revenues, their internal corporate structures, employee numbers, and operational

complexities often resemble those of a medium sized SME organisation rather than a multinational corporation.

- ★ **Limited Headcount for Non-Football Operations:** The core focus of a football club is, inherently, football. The vast majority of staff are dedicated to playing, coaching, scouting, medical, and matchday operations. Departments like IT, digital marketing, data analytics, and cybersecurity often have significantly smaller teams compared to a similarly revenue-generating company in, say, technology or finance. A club with a £500 million turnover might only have a few hundred full-time employees, whereas a global tech firm of similar revenue might have thousands.
- ★ **Prioritization of "Core Business":** Investment and talent attraction tend to flow towards areas directly impacting on-pitch performance. Digital transformation, data infrastructure, and cybersecurity, while critical for long-term sustainability, are often viewed as secondary or "back-office" functions, leading to under-investment.
- ★ **Reliance on Generalists and Outsourcing:** Due to limited headcounts, IT staff often wear many hats, lacking deep specialization in areas like data architecture or advanced cybersecurity. Clubs may outsource digital development or security, but without strong internal oversight and expertise, they struggle to manage these complex relationships effectively or integrate disparate systems.
- ★ **Lack of Corporate Infrastructure & Processes:** Compared to established global corporations, football clubs may lack the mature corporate governance, standardized processes, and extensive internal resources necessary to manage a global digital footprint, complex data strategies, and robust cybersecurity operations. They are "punching well above their size" in the digital sphere without the internal muscle to support it.

This SME paradox means that while Premier League clubs present a polished, global facade to the world, their internal digital and security capabilities are often constrained by the realities of their operational scale. This structural limitation directly contributes to their inability to fully leverage their fan base and leaves them acutely vulnerable to modern cyber threats.

The Path Forward: Scoring in the Digital Age – Securely and Strategically

To unlock the immense potential of their billion-strong social media following, mitigate escalating cyber risks, and overcome their inherent SME-scale operational limitations, Premier League clubs must undergo a fundamental shift in their digital strategy and foundational security posture. This involves:

1. **Building a Unified Fan ID and Data Lake (Securely & Scalably):** Implementing a robust Customer Data Platform (CDP) or similar solution that aggregates all fan data from every touchpoint – social media, website, app, ticketing, retail, email, surveys. Crucially, this must be built with "security by design," meaning cybersecurity considerations are integrated from the very outset of requirements definition, planning and development, not as an afterthought. This provides a single, 360-degree view of each fan.

2. **Developing a Value Exchange Proposition (with Data Privacy as a Cornerstone):** Clubs must offer compelling reasons for fans to provide their first-party data. This includes:
    - **Exclusive Content & Personalized Experiences:** Early access to behind-the-scenes footage, personalized news feeds, and merchandise recommendations.
    - **Transparency and Control:** Clearly communicating what data is collected, why it's collected, how it's used, and giving fans easy control over their data preferences. Building trust through transparent privacy policies is paramount.
    - **Loyalty Programs & Gamification:** Gamified loyalty programs that reward engagement with unique immersive experiences, discounts, or digital collectibles, all built on secure platforms.

3. **Investing in Secure DTC Digital Products (Strategically & Incrementally):** Moving beyond basic websites, clubs need to develop sophisticated DTC platforms and apps that offer premium, secure experiences. This means:
    - **Robust Authentication & Access Controls:** Implementing multi-factor authentication (MFA) for fan accounts and strict access controls to sensitive fan data.
    - **Regular Security Audits & Penetration Testing:** Continuously testing their digital platforms for vulnerabilities.
    - **Secure Payment Gateways:** Ensuring all online payment processing adheres to the highest security standards (e.g., PCI DSS compliance).
    - **Modular Development:** Adopting an agile, modular approach to digital product development that allows for smaller, more manageable projects, aligning with SME operational capabilities.

4. **Strategic Social Media Management (with Security & Data Capture in Mind):** Social media should be seen as a funnel to drive fans to club-owned platforms where first-party data can be captured securely. This means:
    - **Clear Calls to Action (CTAs) to Secure Channels:** Directing fans to official, secure club websites or apps for sign-ups and purchases.
    - **Brand Protection & Impersonation Detection:** Actively monitoring social media for fake accounts or phishing attempts that leverage the club's brand.
    - **Cybersecurity Awareness for Staff:** Training social media managers and all staff to identify and report suspicious activity.

5. **Robust Data Analytics and Personalization at Scale (with Security Best Practices & Managed Services):** Hiring or training data scientists and marketing professionals who can analyze first-party data to segment fan bases, identify high-value segments, and deliver hyper-personalized content and offers, all while adhering to data privacy regulations and security protocols. Given SME limitations, strategic partnerships with data analytics firms or utilizing advanced, cloud-based CDP platforms that offer built-in analytics can bridge the talent gap.

6. **Strategic Investment in Cybersecurity Talent and Infrastructure (Prioritized & Pragmatic):** This is perhaps the most critical, yet often neglected, area.
    - **Appointing a Dedicated CISO (or Fractional CISO):** A senior leader with ultimate responsibility for cybersecurity strategy and implementation, reporting directly to the board. For SME-sized clubs, a fractional CISO (a CISO shared across multiple organizations) or a strong security leader with executive backing can be a pragmatic start.
    - **Building a Cybersecurity Team (or Leveraging Managed Services):** Investing in a small, highly skilled internal team for critical functions, complemented by strategic partnerships with specialized managed security service providers (MSSPs) for 24/7 monitoring, incident response, and threat intelligence. This allows clubs to punch above their weight in cybersecurity.
    - **Implementing Advanced Security Technologies (Cloud-Native & Automated):** Deploying solutions like Security Information and Event Management (SIEM), Endpoint Detection and Response (EDR), and Cloud Security Posture Management (CSPM) to proactively detect and respond to threats.
    - **Regular Cybersecurity Training:** Comprehensive, ongoing training for all employees on phishing awareness, data handling, and secure practices.
    - **Incident Response Planning:** Developing and regularly testing a robust incident response plan to minimize the impact of any breach.

    - **Supply Chain Security:** Vetting third-party vendors for their cybersecurity posture and ensuring contractual obligations around data protection.

7. **Cross-Industry Learning and Collaboration (Targeted):** Premier League clubs should actively learn from best practices in retail, travel, entertainment, and banking, particularly regarding their advanced cybersecurity frameworks and data privacy strategies. Partnerships with digital transformation agencies or sports centric consulting firms can bring in much-needed external expertise, including cybersecurity specialists, guiding them within their operational constraints.

Conclusion

The Premier League's top nine clubs stand at a critical juncture. Their unparalleled global social media reach represents a goldmine of potential, but it remains largely untapped due to a significant deficit in first-party data. The illusion of influence, fueled by massive follower counts, masks a fundamental failure to convert passive engagement into active, repeatable, monetizable fan relationships. By comparison, industries like retail, travel, entertainment, and banking have demonstrated how a strategic focus on first-party data, coupled with compelling DTC offerings and sophisticated personalization, can unlock immense customer lifetime value.

Crucially, the ambition for digital transformation in these clubs is severely hampered by immature cybersecurity operations and a critical lack of dedicated talent. This vulnerability not only undermines trust and hinders the development of secure, personalized digital offerings but also exposes these global brands to escalating business risks from increasingly sophisticated, AI-augmented cybercriminals. This challenge is fundamentally compounded by the SME-like operational scale of these clubs, despite their global brand reach and high revenues. Their limited corporate headcount, prioritization of on-pitch performance, and often generalist IT teams make it incredibly difficult to implement the complex data and cybersecurity strategies required to thrive in the modern digital landscape.

The challenge is not merely technical; it requires a cultural shift within these clubs, prioritizing digital transformation, data literacy, and a fan-centric approach to monetization, underpinned by a robust and proactive cybersecurity posture that acknowledges and strategically addresses their unique operational footprint. The roar of a billion social media followers should not be an echo in an empty digital stadium, but a clear call to action, driving clubs to score the much-needed goals in the burgeoning digital economy. Failing to do so risks leaving billions of pounds on the table and, more importantly, failing to build truly sustainable and deeply engaged relationships with the fans who are the very lifeblood of the beautiful game, all while increasingly falling victim to the unseen hand of cybercrime.

About the Author:

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.