INSIGHTS REPORT

AI’s Dark Play:
No More Sidelines for the C-suite

TIAKI

The Escalating Unseen Threat in Sport

The roar of the crowd, the adrenaline fueled thrill of victory, the precious camaraderie of competition – the global sports industry thrives on passion and connection. But beneath the glittering surface, a silent and insidious battle is raging.

Cybercriminals, increasingly leveraging the power of Artificial Intelligence (AI), specifically Large Language Models (LLMs) like those powering ChatGPT (OpenAI), Gemini (Google DeepMind), Grok (xAI), and DeepSeek LLM (DeepSeek AI), are targeting sports organizations, athletes, and fans with sophisticated ransomware and deepfake attacks.

The period of 2023, 2024, and early 2025 has provided some stark examples of how cybercrime is becoming a formidable challenge, impacting sports properties, regulators, broadcasters, and the critical ticketing supply chain across the globe.

The Rise of AI-Powered Ransomware in Sport: Holding the Game Hostage

Ransomware, the digital equivalent of kidnapping data and demanding a payout, has been a persistent threat for years. However, the advent of advanced AI tools has given cybercriminals an unprecedented advantage, making these attacks more targeted, faster, and devastating-at-scale. In the sports industry, this translates to disruptions that can impact everything from ticketing systems and player management to broadcast schedules and fan engagement.

Automated Reconnaissance and Phishing:
LLMs are being weaponized to conduct highly effective reconnaissance on sports organizations. By sifting through vast amounts of publicly available data – news articles, social media profiles of executives, public filings – these AI tools can identify key personnel, organizational structures, and potential vulnerabilities. This intelligence then feeds into the creation of hyper-realistic phishing campaigns.

In the last 2 years, we've seen a surge in phishing emails that are almost indistinguishable from legitimate communications. AI-generated emails can perfectly mimic the tone, style, and even specific jargon of a sports league, team, or vendor. This makes it incredibly difficult for employees, even those with cybersecurity training, to detect the fakes. Once an employee clicks a malicious link or opens an infected attachment, the ransomware payload can be delivered, encrypting critical data and bringing operations to a standstill.

Targeted Extortion and "Triple Extortion":
The nature of ransomware has evolved beyond simply encrypting data. Cybercriminals are now employing "triple extortion" tactics, which AI aids in escalating. Beyond demanding a ransom for data decryption, they threaten to:

1. **Leak sensitive information:** AI-powered analysis can quickly identify and categorize sensitive data stolen during an attack, such as player contracts, financial records, fan databases, or proprietary training strategies. The threat of public disclosure – a major blow to reputation and a potential violation of data privacy regulations (like GDPR) – puts immense pressure on sports organizations to pay quickly.

2. **Launch DDoS attacks:** If the initial ransom isn't paid, AI-orchestrated Distributed Denial-of-Service (DDoS) attacks can be unleashed, overwhelming a sports organization's websites or online

services.

3. **Target partners and customers:** AI can be used to identify and target an organization's partners, sponsors, and even fans with further phishing or extortion attempts, amplifying the pressure.

Real-World Examples of Ransomware & Data Breaches (2023 - May 2025):

★ **Bologna FC (European Football, Italy, November 2024):** The Italian Serie A football club, Bologna FC, experienced a significant ransomware attack by the RansomHub group. The attackers claimed to have exfiltrated over 200 gigabytes of sensitive data, including sponsorship contracts, the club's complete financial history, personal and confidential player data (including medical records), transfer strategies, and confidential data of fans and club employees. The threat actors even leveraged potential GDPR violations as a tactic to pressure the club into paying the ransom. While the club's immediate operational systems remained unaffected, the public revelation of the data theft, and the subsequent leak of some data on the dark web, highlighted the severe reputational and legal consequences for a prominent European football property.

★ **Grand Palais Olympic Venue (European Sports Infrastructure, Paris, 2024 Olympics):** During the extensive cybersecurity preparations for the 2024 Paris Olympics, a ransomware attack targeted the Grand Palais Olympic venue. French authorities and cybersecurity agency ANSSI (Agence Nationale de la Sécurité des Systèmes d'Information) confirmed the incident. While this specific attack did not directly disrupt Olympic activities or main IT systems, it underscored the persistent and pervasive threat of ransomware even against highly fortified targets within the broader sports ecosystem, particularly major event infrastructure. It served as a stark reminder that no critical sporting asset is entirely immune.

★ **Aston Villa FC (European Football, UK, 2024):** Aston Villa Football Club inadvertently exposed a publicly accessible Amazon Web Services (AWS) S3 bucket containing personally identifiable information (PII) of approximately 135,770 individuals. The leaked data included full names, dates of birth, home addresses, phone numbers, email addresses, membership details, and purchase information. This exposure, while not a direct ransomware attack, increased the risk of spear phishing and social engineering attacks for the affected fans, demonstrating how vulnerabilities can be exploited for subsequent attacks.

★ **Liverpool FC (European Football, UK, July & November 2024):** Online sales for Liverpool FC members were subjected to a cyberattack in July and November 2024. The target was illegally harvested tickets, highlighting a direct attack on a club's revenue stream and fan experience. While specifics on the type of attack are not always disclosed, such incidents often involve sophisticated phishing or credential stuffing, potentially enhanced by AI.

The Deepfake Deluge: Eroding Trust and Spreading Misinformation in Sport

Deepfake technology, once a niche curiosity, has rapidly advanced with the help of generative AI. These hyper-realistic fabricated videos, images, and audio recordings pose a severe threat to the integrity and reputation of the global sports industry. Since 2023, the concerns surrounding deepfakes shifted from theoretical to alarmingly real.

Sophisticated Deepfake Scams and Endorsements:
LLMs are instrumental in creating the convincing scripts and narratives behind deepfake scams. They can analyze vast amounts of text and audio from public figures, including athletes and sports executives, to generate incredibly natural-sounding speech and highly realistic facial expressions.

Such deepfakes can be used for:

- ★ **Financial scams:** Impersonating sports figures or executives to solicit investments in fake schemes, trick employees into transferring funds.

- ★ **Reputational damage:** Creating fabricated videos of athletes or officials engaging in unethical or controversial behavior, leading to widespread public outcry and damage to personal and organizational brands, which directly destroys immediate monetisation opportunities for the impacted parties.

- ★ **Disinformation campaigns:** Spreading false narratives to manipulate public opinion, influence betting outcomes, or discredit rival teams or organizations.

Real-World Examples of Deepfakes and Disinformation (2023 - May 2025):

- ★ **Ronaldo Nazário Deepfake Endorsement (Global Football, September 2024):** A highly publicized incident in September 2024 involved an AI-manipulated video that appeared to feature retired Brazilian football legend Ronaldo Nazário. In the deepfake, he was seen endorsing an online game and encouraging users to download a specific app. Although the video contained some visual and audio inconsistencies, its initial appearance was convincing enough to deceive many casual viewers. This case served as a stark warning about the immediate threat of deepfake endorsements for fraudulent financial scams, leveraging the immense trust and influence that sports icons hold globally.

- ★ **Paris 2024 Olympics Disinformation Campaigns (Global Sports, 2024):** The 2024 Paris Olympics were a major target for sophisticated disinformation campaigns, some of which reportedly leveraged AI-generated content. State-affiliated actors and other malicious entities aimed to tarnish France's image and question its preparedness through false claims, amplified by bot activity and coordinated social media narratives. For instance, AI-generated videos portraying Paris as crime-ridden were circulated to mock the Games' security preparations, impacting public perception and potentially attendance. These efforts highlight how AI assists in creating and disseminating compelling false narratives to influence public opinion around major sports events, affecting both the event organizers and indirectly, their broadcasting partners.

- ★ **Deepfake Voice Fraud Attempt (Global, Early 2024 - Arup Case):** While not sports-specific, the case of Arup, a global engineering firm, losing over $25 million in early 2024 due to deepfake voice technology underscores the immediate threat to any high-value target in any industry, including sports organizations with significant financial transactions. A finance employee was tricked into transferring funds after participating in a video conference call with deepfaked voices of senior executives. This shows how AI-powered voice and video impersonation can be used to target executives within sports properties, leagues, or broadcasting companies.

The Interplay: LLMs as the Brains Behind the Brawn

It's crucial to understand that ChatGPT, Gemini, Grok, DeepSeek and other LLMs aren't directly executing

ransomware or creating deepfake videos themselves. Instead, they act as the "brains" that empower cybercriminals to execute these attacks with greater efficiency, scale, and sophistication.

Here's how LLMs contributed to the attacks witnessed in 2023-2025:

- ★ **Content Generation:** Crafting highly convincing phishing emails, social engineering scripts, and deceptive narratives for deepfake scenarios. They can adapt their language and tone to target specific individuals or organizations within the sports industry, such as sports agents, club officials, broadcasting executives, or even employees of ticketing companies.

- ★ **Code Generation:** While not directly generating malicious payloads, LLMs can assist in writing code for various components of an attack, such as automating reconnaissance scripts or improving the efficiency of data exfiltration tools used in ransomware campaigns.

- ★ **Information Synthesis:** Quickly analyzing vast amounts of data to identify vulnerabilities, compile lists of potential targets, and understand the internal workings of sports organizations, regulators, broadcasters, and ticketing entities to craft more effective attacks. This includes sifting through public records of sports federations, league rules, broadcasting schedules, and even ticketing terms and conditions to find opportune moments for disruption.

- ★ **Scaling Operations:** Enabling threat actors to launch attacks on a much larger scale, generating unique phishing messages or deepfake variations for hundreds or thousands of targets simultaneously, bypassing traditional security filters. This is particularly relevant for large-scale events like the Olympics or major tournaments, where the attack surface is enormous.

Impact on North American Leagues, Sports Regulators, and Broadcasters

While specific "ransomware" attacks directly impacting NFL, NBA, MLB, NHL, or MLS league operations were not widely publicized during this period, these leagues consistently face a barrage of sophisticated cyber threats, with AI enhancing the capabilities of attackers.

- ★ **Credential Compromise (North American Leagues, Ongoing 2023-2025):** Cybersecurity reports from 2023, 2024, and early 2025 highlighted the alarming number of compromised passwords related to popular North American sports teams. For instance, data analysis revealed that passwords including "New York Yankees," "Dallas Cowboys," "Oklahoma City Thunder," and "New York Rangers" were among the most frequently leaked in data breaches. While these are often consequences of broader credential stuffing attacks (where stolen credentials from one breach are tried on other sites), AI tools are increasingly used to automate and scale these brute-force attempts. This poses a direct threat to league and team staff accounts, fan databases, and potentially internal systems if multi-factor authentication is not universally enforced.

- ★ **FIFA Player Contract Data Theft (Global Regulator, Pre-2023 but relevant context):** While the most prominent incident regarding FIFA's player contract data theft occurred prior to 2023 (specifically around 2018-2019, exposed through "Football Leaks"), it remains a critical example of the type of sensitive data held by sports regulators and the severe consequences of its breach. The stolen data included confidential emails between FIFA officials, member associations, and legal teams, detailed strategies related to bidding processes, and crucially, personal information about players, including contract details and private communications. This incident serves as a stark reminder of the immense value of data held by global sports regulators like FIFA and how such information could be targeted, now with AI-enhanced methods for reconnaissance and exfiltration.

Ongoing state-sponsored activities, such as APT28 (attributed to Russian military intelligence) targeting "a sport organization involved in the 2024 Olympic and Paralympic Games" as reported by the French Ministry for Europe and Foreign Affairs in April 2025, further indicate a persistent, state-sponsored interest in disrupting or discrediting sports governing bodies and stealing sensitive data.

- ★ **DDoS Attack on Online Betting Platform During NHL Event (Global/North American Market, April 2025):** In April 2025, an online bookmaker experienced a massive Distributed Denial-of-Service (DDoS) attack, peaking at 965 Gbps, during a major NHL event – specifically, around the time Alexander Ovechkin was nearing his record-tying goal. While the primary target was a betting site, such large-scale attacks on a platform directly tied to live sporting events demonstrate the capabilities of AI-orchestrated botnets to disrupt services during peak sports moments. Such disruptions could easily spill over to affect official league streaming services, broadcasters' platforms, or even ticketing systems if they share infrastructure or fall under the same attack campaigns. This highlights the vulnerability of the entire digital ecosystem surrounding major North American sports.

- ★ **Polish National Team Broadcast Disruption (European Sports Broadcasting, March 2024):** In March 2024, the online broadcast of Poland's opening Euro 2024 qualification match against Estonia was disrupted. Suspicions quickly pointed towards Russian-linked hackers. While the exact methods aren't always publicly detailed, such disruptions often involve DDoS attacks or targeted network intrusions. This showcases the vulnerability of sports broadcasters to nation-state level cyber warfare, especially during high-profile international matches.

The Vulnerable Sports Ticketing Supply Chain

The sports ticketing supply chain, a complex fragmented web of primary vendors, secondary markets, payment processors, and venue access control systems, presents a particularly attractive and vulnerable target for cybercriminals. Each link in this chain can be exploited, with AI empowering more sophisticated attacks.

Real-World Examples (2023 - May 2025):

- ★ **Sportadmin Data Leak (Swedish Sports Associations, January 2025):** One of Sweden's most significant cybersecurity incidents in early 2025 involved Sportadmin, a platform used by over 1,700 sports associations and managing data for approximately 2 million individuals. This platform often handles member registrations, event sign-ups, and potentially some form of internal club ticketing or access management for smaller sporting events. A data breach, discovered on January 16, 2025, exposed a vast amount of personal data, including names and contact details of sports participants and club members. While the platform's payment functions were unaffected due to external suppliers, the breach underscores the vulnerability of third-party service providers within the broader sports "supply chain" – in this case, a critical administrative one that supports numerous sports activities. This kind of data can be invaluable for highly personalized phishing attacks, potentially leading to further breaches in ticketing or other financial systems.

- ★ **Online Sales for Liverpool FC Members (European Football, July & November 2024):** As mentioned earlier, attacks specifically targeting ticket sales for Liverpool FC members aimed at illegally harvesting tickets. These attacks highlight the direct financial and reputational impact of breaches within the ticketing process. Such attacks often exploit vulnerabilities in online payment gateways or credential management systems.

★ **General Rise in Supply Chain Attacks (Global, 2023-2025):** Cybersecurity reports from 2023-2025 continually emphasize the dramatic increase in "supply chain attacks." Threat actors are increasingly exploiting weak links in third-party vendor networks rather than directly attacking well-defended primary targets. This includes compromised third-party software providers, IT managed service providers (MSPs), or even open-source libraries. For the sports ticketing industry, this means that even if a major ticketing platform has robust defenses, a vulnerability in one of its smaller, less-secure vendors (e.g., a software provider for seating charts, a payment gateway, a digital marketing agency handling fan data, or a physical ticket printer) could be exploited to gain access to critical systems or sensitive fan data. The high value of tickets and fan data makes any weak link in this supply chain a prime target for AI-enhanced reconnaissance and attack.

The Sports Betting Industry: A High-Stakes Target

The sports betting industry is a particularly attractive target due to the large sums of money transacted, the real-time nature of its operations, and its reliance on online platforms. DDoS attacks and ransomware are major concerns.

Real-World Examples (2023 - May 2025):

★ **MGM Resorts and Caesars Entertainment Ransomware (US, September 2023):** These two major casino giants, which often have significant sports betting operations, were hit by high-profile ransomware attacks in September 2023. MGM reported a $100 million impact on its Q3 earnings due to the disruption. These attacks were notably attributed to the notorious cybercriminal group known as **Scattered Spider** (also linked to the **ALPHV/BlackCat** ransomware gang). Their modus operandi involved sophisticated social engineering tactics, often leveraging voice phishing (vishing) to trick IT staff into bypassing multi-factor authentication and gaining initial access.

★ **Recent Retail Attacks by Scattered Spider (UK, April 2025):** In April 2025, a significant wave of cyberattacks hit prominent UK retailers, including **Marks & Spencer, Harrods, and Co-op**, causing widespread disruptions and devastating losses of revenue. Cybersecurity experts have strongly linked these attacks to Scattered Spider, the same group responsible for the MGM Resorts and Caesars Entertainment breaches. The methods employed, such as social engineering against third-party IT service providers (like Tata Consultancy Services in the M&S case) to gain initial access, mirrored their past tactics. M&S, for instance, saw online orders suspended, stock shortages, and an estimated £300 million reduction in profits for the current year due to the incident, demonstrating the crippling financial impact this group can inflict across industries.

★ **International Game Technology (IGT) Cyberattack (Global Betting Tech Vendor, November 2024):** IGT, a major global provider of slot machines and other gambling technology for lottery and sports betting operations, took certain IT systems offline following a cyberattack discovered on November 17, 2024. While the specifics of the attack were not fully disclosed, the proactive shutdown indicates a significant security incident. As a key vendor in the sports betting supply chain, a disruption to IGT could have widespread implications for numerous betting operators worldwide.

★ **Largest DDoS Attack of 2025 on Online Betting Organization (Global, April 2025):** As previously mentioned, a massive DDoS attack reaching nearly 1 Terabit per second targeted an online betting organization during a major NHL event in April 2025. This multivector attack demonstrates the scale and real-time impact that AI-orchestrated botnets can achieve, specifically targeting the highly lucrative and time-sensitive sports betting sector. Similar attack patterns were

noted during the 2024 UEFA European Football Championship, where spikes in DDoS activity also targeted online betting sites.

Mitigating the Threat: A Constant Game of Catch-Up

The rapid evolution of AI-powered cyber threats means the sports industry is in a constant game of catch-up. However, several strategies are being implemented and refined:

- ★ **Enhanced Employee Training:** Recognizing that the human element remains the weakest link, sports organizations, regulators, broadcasters, ticketing companies, and betting operators are investing in advanced cybersecurity training that specifically addresses AI-generated phishing, deepfakes, and social engineering tactics. The success of Scattered Spider, in particular, highlights the critical need to educate employees about sophisticated social engineering.

- ★ **AI for Defense:** Paradoxically, AI is also a powerful tool for defense. AI-driven security systems are being deployed to detect anomalies, identify suspicious patterns in network traffic, and even detect deepfake content in real-time. The **IOC's use of an AI-powered system (Threat Matrix) to monitor social media for online abuse during the 2024 Paris Olympics** is a prime example of AI being used defensively in sports, extending to broader threat detection.

- ★ **Multi-Factor Authentication (MFA) and Zero Trust:** Implementing robust MFA across all systems significantly reduces the risk of account compromise, even if phishing attempts are successful. Adopting a "Zero Trust" security model, where no user or device is inherently trusted, provides additional layers of protection, crucial for complex ecosystems like those of sports broadcasters or event organizers and ticketing platforms handling sensitive financial data.

- ★ **Robust Data Backup and Recovery:** Regular, off-site, and immutable backups are critical to minimize the impact of ransomware attacks, allowing organizations to restore data without paying the ransom.

- ★ **Supply Chain Security Audits:** Given the increasing vulnerability of supply chains, sports organizations are enhancing their due diligence on third-party vendors, particularly those involved in ticketing, data management, and operational technology. This includes regular security audits and contractual requirements for robust cybersecurity measures. The attacks on M&S and Co-op, seemingly through a third-party IT provider, underline this critical need.

- ★ **Collaboration and Information Sharing:** Sports organizations, cybersecurity firms, law enforcement agencies, and even competitors are increasingly collaborating to share threat intelligence and best practices, collectively strengthening defenses against AI-powered cybercrime. This was evident in the widespread information sharing and "cyber war games" conducted in preparation for the Paris 2024 Olympics.

- ★ **Legislation and Regulation:** Governments and international bodies are grappling with how to regulate AI to prevent its malicious use, with ongoing discussions about accountability and ethical guidelines for AI development and deployment. The new UK Cyber Code of Governance published in **April 2025** is one such example, aiming to guide boards and directors on managing cybersecurity risks, a necessity for all organizations, including those in sports.

The Future is Now: A Call to Action

Recent events have demonstrated that AI is not just a tool for innovation; it is a weapon being actively wielded by cybercriminals. The global sports industry, with its high visibility in society impacting our daily lives, large capital investments, valuable fan and player data, and complex operational needs, represents an increasingly attractive target for ransomware and deepfake attacks.

The track record of groups like Scattered Spider in crippling major enterprises across various sectors—including large corporations deeply tied to the sports industry, such as major sports betting platforms, global broadcasters, and leading sports apparel brands, along with significant retail brands—underscores the existential threat.

As LLMs like ChatGPT, Gemini, Grok and DeepSeek continue to advance, the sophistication of AI-powered cyberattacks will only grow. It is no longer enough for sports properties, regulators, broadcasters, ticketing companies, and betting operators to react to threats after the attack; they must proactively invest in cutting-edge cybersecurity, foster a culture of security awareness at all levels, and embrace the defensive capabilities of AI itself. The integrity of the game, the safety of athletes, the trust of fans, and the seamless delivery of sporting spectacles depend on it. The digital dark side of sport is here, and the battle for its future is only just beginning.

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.