The Silent Value Killer: How the AI-powered Cybercriminal Steals Your Sports Fan Data

TIAKI

The AI-Powered Heist: how cybercriminals are targeting sports properties worldwide

The global sports industry, a multi-billion dollar ecosystem built on fan loyalty and high-value data, is facing a new and insidious threat: AI-augmented cybercrime.

Criminals are leveraging the very technology touted for its potential to revolutionize sports to instead bypass outdated cybersecurity defenses and steal confidential fan data, sensitive financial records, and proprietary athlete information. The consequences of such breaches can be catastrophic, eroding trust with fans, investors, ecosystem partners, broadcasters, and sponsors, ultimately decimating a sports property's brand and value creation potential.

.

A cybercriminal, armed with generative AI (GenAI) tools, can exploit vulnerabilities in immature cybersecurity operations at sports properties across North America, Europe, and Asia with alarming ease. Traditional security solutions and operations teams, designed for a pre-AI landscape, are blind to the activity happening within GenAI applications and lack the capability to manage the speed, complexity and scale of an attack. This is creating a ‘perfect storm’ for data exfiltration at sports properties.

AI-augmented cybercriminals smell opportunity in private equity invested franchises with high value rights deals

The cybercriminals are opportunistic and will prioritise soft, easy targets that are digitally and data immature, where there is significant private equity investment and sports rights deal valuations to justify the criminals’ demands for high ransomware payouts following a data breach theft.

The NBA’s $76 billion and NFL’s $111 billion sports rights deals, with increasing amounts of private equity investment and an explicit business goal to target data-driven fan growth in international markets, demonstrates exactly why the sports industry is becoming an increasingly attractive target for ransomware data breach attacks. Similarly, in English cricket, The Hundred 2025 investor auction was ground-breaking, made high profile headlines and raised almost £1 billion into 8 cricket franchises. It will not have escaped the radar of the world’s leading cyber gangs.

The cybercriminals are now ‘AI-weaponised’ to attack enterprises that have failed to put robust network cybersecurity postures in place. The cost of a data breach is significant. Our research suggests $6.1 million was the average cost of an enterprise data breach based on 200 selected enterprises with high-end monitoring [1]. In addition the risk of unrepairable brand damage for the sporting entity, the loss of trust from sporting fans and athletes from the theft of their personal data, and the exit of sponsors and investors, could quickly create an untenable, unrecoverable business.

[1] Orange Cyberdefense Security Navigator Report 2024: Research-based cybersecurity insights to drive smart business decisions

Low cybersecurity maturity and lack of C-suite governance makes sport the easy target

As the 'AI-weaponised' cybercriminals ramp up the volume and complexity of their data breach attacks, the cyber threat and consequential risks to new 2025 sporting business models have never been higher. The industrialisation of the cybercriminal ecosystem has created a **79% increase in ransomware attacks in the last 12 months[2].**

Attacks are happening faster than organisations can respond, across all sectors, which justifies growing C-suite anxiety on the risk to the sports industry. The average number of days for the cybercriminal to gain access to an enterprise and then extract data was 44 days in 2021 and reduced to 5 days in 2023. In 2025 this can now be done in a matter of hours [3].

Our research confirms that **80% of data breaches occurred on cloud assets in the last 12 months**. Cybercriminals are constantly looking for vulnerabilities in these digital platforms to exploit and launch ransomware attacks.

One of the factors that make the sports industry particularly vulnerable to ransomware attacks is the low maturity of Secure Access Service Edge (SASE) solutions. SASE combines network security functions with wide-area networking capabilities to provide a comprehensive security solution for organisations. However, many sports organisations have not fully implemented or optimised their SASE frameworks, leaving them exposed to cyber threats and data breaches. This lack of maturity in SASE capability, combined with lack of digital-data-AI guard rails and governance from the C-suite in sports properties, makes it easier for cybercriminals to infiltrate sports franchises and launch ransomware attacks.

Worryingly, despite the billion dollar sports rights deals, only **30% of sporting organisations have a robust digital strategy in place[4] and only 5% of enterprises have defined their SASE strategy.** It seems clear that C-suite executives are not yet receiving appropriate strategic advice or taking ownership for their potential cybersecurity exposures.

Consequently the risk of a catastrophic ransomware data breach attack has never been higher to the broad array of sporting entities in the digital sporting value chain.

A Cybercriminal's Playbook

Imagine a scenario where a malicious actor uses the following techniques to penetrate a sports organization's defenses:

- ★ **Social Engineering with AI:** Employees, often unknowingly, become unwitting accomplices. Cybercriminals can craft highly convincing phishing attacks, personalized with information gleaned from AI-powered reconnaissance, to trick employees into pasting sensitive data, such as

---

[2] Orange Cyberdefense Executive Navigator 2024: Research-based cybersecurity insights to drive smart business decisions

[3] PaloAlto Unit 42 Cloud Threat Report, Volume 7: Navigating the Expanding Attack Surface

[4] www.isportconnect.com/impact-of-digital-transformation-on-sporting-organizations/

fan PII, contract details, or financial reports, into seemingly innocuous AI chatbots. The trust employees place in these tools becomes a vulnerability.

- ★ **Data Loss Prevention (DLP) Bypass:** Traditional DLP tools struggle to inspect browser-based AI interactions. This allows sensitive data to flow freely into AI applications, bypassing established security protocols. Today, employees are spending 85% of their time in the workplace in browser based activities, so this is a significant risk[5].

- ★ **AI-Powered Data Aggregation:** Large Language Models (LLMs) can be trained to capture and index leaked data from multiple employees. This creates a centralized repository of stolen information, easily searchable and exploitable by the criminal.

- ★ **Prompt Engineering for Data Recovery:** Even if employees attempt to delete sensitive information, sophisticated prompt engineering can be used to extract insights from previous user interactions stored within the AI system, effectively resurrecting seemingly deleted data.

- ★ **Cloaking within the System:** Security Operations Centers (SOCs) often lack visibility into AI query logs. This allows cybercriminals to operate undetected, exfiltrating data without leaving a trace in traditional security information and event management (SIEM) systems. Many sports properties are under-invested in cybersecurity operations and do not even have a SOC in place. This further heightens their critical vulnerabilities and exposure to an AI-powered data breach.

Why This Works

This alarming scenario is effective due to several factors:

- ★ **AI Trust Blindness:** Employees often trust AI tools implicitly, failing to recognize the risks of exposing sensitive data.

- ★ **Outdated Security Stacks:** Current security infrastructure is not designed to monitor real-time LLM interactions, leaving a critical blind spot.

- ★ **Security Information & Event Management (SIEM) Gaps**: SIEM systems are often not configured to log GenAI activity, allowing data exfiltration to occur without triggering alerts.

The Catastrophic Risks

The potential consequences for sports properties are severe:

- ★ **Massive Data Breaches:** Leaked Personally Identifiable Information (PII) of fans, including names, addresses, financial details, and even health information, can lead to reputational damage, increased churn rates, legal action, and significant financial penalties.

- ★ **Financial Losses:** Stolen financial data, including proprietary revenue figures, sponsorship deals, and budget information, can be used for competitive advantage or even lead to direct

[5] Embrace the Browser-Driven Workspace - Palo Alto Networks

financial theft.

- ★ **Athlete Data Exposure:** Sensitive athlete data, including medical records, performance metrics, and contract details, can be exploited for blackmail, competitive advantage, or even put athletes at risk.

- ★ **Erosion of Trust:** Data breaches erode trust with fans, sponsors, investors, and other stakeholders, leading to decreased revenue, loss of partnerships, and a significant decline in brand value.

Your Defence

Sports properties must take immediate action to protect themselves in 2025:

- ★ **Enterprise-wide SASE Strategy**: Define and implement an holistic SASE strategy across the entire sports organisation with active C-suite sponsorship and leadership. Give ownership and accountability for the SASE strategy to the Chief Data Officer or Chief Revenue Officer. It is a revenue multiplier not a cost burden. It must be closely coupled with the digital strategy, data strategy and business strategy. Get industry leading strategic advice on what good looks like. Make SASE a board level agenda item so that it receives the appropriate level of investment prioritisation to robustly protect data assets for digital data monetisation.

- ★ **Data Redaction:** Implement systems that automatically redact sensitive data before it reaches the LLM.

- ★ **GenAI App Control:** Utilize advanced browser security controls to block access to risky GenAI applications.

- ★ **AI Interaction Logging:** Integrate AI interaction logs into SIEM systems for real-time threat detection.

- ★ **Robust Security Policies:** Develop and enforce strict security policies regarding the use of AI tools by employees.

Potential for highly damaging ransomware attacks

Given the increasing digitalization of the sports industry, the recent $ billion+ sports rights deals, and the low maturity of SASE solutions, there is a significant risk that the industry could experience highly damaging ransomware attacks in the next 18 months.

Cybercriminals are constantly evolving their tactics and targeting organisations who possess valuable data and content. The sports industry, with its vast amount of valuable ‘game day’ content and sports fan data, is an increasingly lucrative, prime target for ransomware attacks. If these attacks were to occur, they could have devastating consequences for sports leagues, sports properties and sports broadcasters, leading to data breaches, financial losses, and huge reputational damage.

The time to act is now.

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.