BLOG REPORT

Beyond the Boundary: Why Cybersecurity is the Next Big Score in The Hundred and IPL

TIAKI

The Silent Match: How Cybercriminals Target The Hundred and IPL Crown Jewels

The thud of bat on pad, the abrasive roar of ‘howzat’, the electrifying tension of a final over, — these are the hallmarks of cricket's most thrilling spectacles in The Hundred and the Indian Premier League (IPL). Yet, beyond the pitch and the passionate cheers, a covert, high-stakes battle is unfolding in the digital world. This unseen contest involves immense financial transactions, the sensitive personal data of players and fans, and the intricate digital systems that power everything from live broadcasts to ticket sales. In this arena, **cybersecurity isn't merely a defensive stance; it's the strategic play for the next big win.**

A particularly insidious and growing new threat, the malicious use of **residential proxy services**, presents a significant risk that cybercriminals are eager to exploit in these high-stakes cricket environments.

Understanding the Threat: Residential Proxies as a Criminal Camouflage

For years, cybercriminals relied on "bulletproof" hosting services to maintain anonymous web infrastructure. However, with increasing scrutiny and improved law enforcement strategies, criminals have pivoted dramatically, now heavily leveraging **residential proxy networks**. These services route malicious traffic through legitimate consumer devices (e.g., home computers, smart devices) with rotating IP addresses assigned to homes and offices.

The key danger lies in this camouflage: traffic originating from a residential proxy appears as everyday online activity. This makes it incredibly difficult for security systems to distinguish between legitimate user behavior and malicious actions, allowing criminals to evade detection and operate under the radar. The decentralized nature of these platforms also makes it challenging for service providers to control their use, further hindering law enforcement's ability to trace and apprehend perpetrators.

Exploitation in The Hundred & IPL Cricket Leagues: A Multi-Faceted Risk

The unique characteristics of The Hundred and IPL Cricket Leagues—their global reach, high fan engagement, reliance on digital platforms, and significant financial transactions—make them particularly vulnerable to exploitation via residential proxies:

- ★ **Evading Anti-Bot and Fraud Detection Systems (Ticketing & Merchandise):**
  - **Ticket Scalping and Bots:** Cybercriminals can use residential proxies to bypass IP-based rate limits and anti-bot measures on official ticketing websites. By rotating through thousands of seemingly legitimate residential IP addresses, they can rapidly purchase large quantities of tickets, leading to price gouging on secondary markets and depriving genuine fans.
  - **Merchandise Fraud:** Similarly, bots powered by residential proxies can exploit limited-edition merchandise sales, buying up stock to resell at inflated prices, or even engage in credit card fraud by testing stolen card numbers across e-commerce platforms.

- ★ **Credential Stuffing and Account Takeovers (Fan & Player Accounts):**
  - **Fan Accounts:** Many fans register accounts for streaming services, fantasy leagues, and official team apps. Criminals can use residential proxies to launch large-scale credential stuffing attacks, where stolen username/password combinations from other breaches are tried against these platforms. The residential IPs make these attempts appear like legitimate user logins, making detection difficult. Successful takeovers can lead to access to personal information,

payment details, or even the ability to spread misinformation.
    - **Player and Staff Accounts:** Even more critically, accounts belonging to players, coaches, and league staff are high-value targets. If compromised via credential stuffing or targeted phishing campaigns (where residential proxies mask the origin of the attack), criminals could gain access to sensitive strategic information, financial data, or even the ability to disrupt operations.

★ **DDoS Attacks and Infrastructure Disruption:**
    - While not always the primary method for large-scale DDoS, residential proxies can be part of a sophisticated botnet used to launch distributed denial-of-service (DDoS) attacks. By flooding league websites, streaming platforms, or online betting sites with traffic from thousands of legitimate-looking IPs, criminals could disrupt services, cause outages during critical match times, or even extort organizations by demanding ransom to stop the attacks.

★ **Content Piracy and Geo-Restriction Bypass:**
    - **Illegal Streaming:** Residential proxies can be used to bypass geo-restrictions on legitimate streaming services, allowing unauthorized access to live matches and copyrighted content. This directly impacts revenue streams for broadcasters and the leagues themselves.
    - **Content Scraping:** Criminals might also use these proxies to scrape data from official websites, potentially for illicit purposes like creating fake news or phishing sites.

★ **Malware Distribution and Phishing Campaigns:**
    - Residential proxies can serve as an anonymous backbone for distributing malware or hosting phishing sites. Links distributed through social media or email that lead to malicious content can have their origin masked by these proxies, making it harder for security teams to trace the source of the infection or fraudulent activity.

The CEO Imperative of Proactive Cybersecurity: Beyond Compliance and Cost Centres

In the rapidly evolving digital landscape, cricket franchises and their leadership can no longer afford to treat cybersecurity as a mere reactive measure, a burdensome cost, or a checkbox for regulatory compliance. The stakes are simply too high. Cybersecurity must be recognized and actively championed by the CEO and the entire C-suite as an integral part of digital revenue enablement, deeply connected with the organization's data and overarching business strategy to drive growth.

Delegating cybersecurity solely to IT or treating it as a priority only *after* a cyberattack or a compliance failure is an unacceptable risk. Such an approach puts the entire business in jeopardy, threatening brand reputation, fan trust, financial stability, and operational continuity. The appropriate level of investment, aligned with growth ambitions, is not merely a defensive expenditure but a strategic enabler.

The CEO must own cybersecurity. This means:

★ **Strategic Visionary:** Articulating a clear vision for cybersecurity that aligns with the franchise's digital transformation and revenue goals.

★ **Active Champion:** Proactively ensuring best practices are ingrained across the organization and fostering a culture where security is everyone's responsibility.

★ **Resource Allocator:** Ensuring that the appropriate financial and human capital investments are made to build a resilient data and cybersecurity operation, not just to meet minimum compliance

requirements.

- ★ **Risk Manager:** Understanding the top cyber risks to the business and demanding clear mitigation strategies, rather than waiting for a breach to highlight vulnerabilities.
- ★ **Communicator:** Being comfortable with the vocabulary of cybersecurity, data, and AI, and leading discussions at leadership meetings to ensure continuous improvement and adaptation to new threats.

This top-down commitment transforms cybersecurity from a reactive cost burden into a proactive strategic asset that safeguards and accelerates digital revenue growth.

Additional Considerations for a Resilient Cricket Franchise

To truly safeguard against the evolving threat landscape, including the sophisticated tactics enabled by residential proxies and emerging AI-augmented threats, cricket franchises must adopt a comprehensive and proactive cybersecurity posture.

1. Embracing a SASE Strategy and Benchmarking Maturity

A fundamental shift is required towards a **Secure Access Service Edge (SASE)** architecture. SASE converges networking and security functions into a single, cloud-delivered service, providing consistent security policies and performance for all users, regardless of their location. For a globally distributed entity like a cricket franchise, with remote players, staff, and a vast fan base accessing services from diverse locations, SASE offers immense benefits:

- ★ **Unified Security:** Integrates key security functions like Secure Web Gateway (SWG), Firewall-as-a-Service (FWaaS), Cloud Access Security Broker (CASB), and Zero Trust Network Access[1] (ZTNA).
- ★ **Enhanced Performance:** Optimizes access to cloud applications and resources, reducing latency.
- ★ **Simplified Management:** Reduces complexity by consolidating multiple security tools into one platform.
- ★ **Scalability:** Easily scales to accommodate fluctuations in user numbers and data traffic, crucial during peak season.

The cricket franchise should conduct a **SASE maturity benchmark** on its existing operations. This involves assessing current network and security infrastructure, identifying gaps in SASE adoption, and developing a phased roadmap for implementation. This benchmark will highlight where the organization stands in terms of cloud-native security and what steps are needed to achieve a robust SASE framework, ensuring secure and efficient access for all stakeholders from any location.

2. Integrating Data, AI, and Cybersecurity with Business Strategy

As highlighted above, cybersecurity can no longer be an afterthought or a standalone IT function. It must be **deeply interwoven with the business and digital strategy** of the cricket franchise. This means:

- ★ **Strategic Alignment:** Defining a mature data, AI, and cybersecurity strategy that directly supports the franchise's digital revenue growth ambitions, fan engagement goals, and operational efficiency.

- ★ **Investment Justification:** Clearly demonstrating how cybersecurity investments protect and enable new revenue streams (e.g., secure online ticketing, fan data monetization, digital sponsorships) rather than being perceived solely as a cost center.

- ★ **Risk-Based Approach:** Prioritizing cybersecurity initiatives based on a clear understanding of the business impact of potential cyber threats. This ensures that appropriate levels of investment are made where they matter most.

- ★ **Data Governance:** Establishing robust data governance frameworks to manage the vast amounts of fan data, player performance data, and financial information, ensuring its security, privacy, and ethical use, especially in the context of AI applications.

3. Cultivating C-Suite and Board Cybersecurity Fluency and Ownership

For any comprehensive cybersecurity strategy to succeed, **C-suite executives and board members must be comfortable with the vocabulary of cybersecurity, data, and AI**. Their active participation and ownership are paramount:

- ★ **Strategic Dialogue:** Leaders should be able to discuss cyber risks and opportunities in business terms, understanding the potential impact of breaches on reputation, revenue, and regulatory compliance.

- ★ **Proactive Ownership:** Beyond merely approving budgets, the C-suite should actively champion best practices, foster a security-first culture, and ensure continuous improvement in the franchise's data and cybersecurity operations.

- ★ **Risk Appetite:** Defining the organization's acceptable risk appetite for various cyber threats and ensuring that security measures align with these parameters.

- ★ **Incident Preparedness:** Actively participating in tabletop exercises and understanding incident response plans to ensure swift and effective action in the event of a breach.

4. Leveraging Best-in-Class Technology and Managed Services

To combat the escalating complexity and scale of AI-augmented threats, cricket franchises should **select market best practice cybersecurity technology vendors** such as Palo Alto Networks. These vendors offer comprehensive, AI-powered security platforms designed to detect and prevent advanced threats.

Furthermore, considering **co-managed or fully outsourced cybersecurity managed services** is a strategic imperative. This approach allows the franchise to:

- ★ **Access Specialized Talent:** Tap into a pool of highly skilled cybersecurity professionals who are constantly updated on the latest threats and technologies, addressing the industry-wide talent shortage.

- ★ **Benefit from Best Practices:** Leverage the experience and expertise of a dedicated security partner that manages security for multiple organizations, bringing battle-tested processes and intelligence.

- ★ **Achieve Scale and 24/7 Coverage:** Cope with the immense scale of data and attack surfaces, especially during peak season, and ensure continuous monitoring and rapid response capabilities around the clock.

- ★ **Combat AI-Augmented Threats:** Managed service providers are often equipped with advanced threat intelligence, AI-driven detection tools, and specialized expertise to identify and neutralize sophisticated attacks like those involving residential proxies and deepfakes more effectively than an in-house team might alone.

5. Addressing AI-Augmented Deepfake Threats in the Ticketing Supply Chain

The cricket ticketing supply chain is particularly vulnerable to **AI-augmented deepfake threats**. Deepfakes, synthetic media generated by AI, can create highly convincing fake audio, video, or images that mimic real individuals or organizations. This poses several risks:

- ★ **Fraudulent Endorsements and Promotions:** Deepfake videos or audio of players, coaches, or league officials promoting fake ticket sales or unauthorized merchandise could trick fans into purchasing illegitimate items, leading to financial loss and reputational damage.

- ★ **Phishing and Social Engineering:** Deepfake voices of known contacts (e.g., a manager's voice for a finance executive) could be used in highly targeted social engineering attacks to manipulate employees within the ticketing supply chain into revealing sensitive information or authorizing fraudulent transactions.

- ★ **Counterfeit Tickets:** While not directly creating physical tickets, deepfakes could be used to generate highly believable fake confirmation emails, QR codes, or digital passes that mimic official league communications, leading to fans being denied entry at venues.

- ★ **Disinformation Campaigns:** Deepfakes could be used to spread false information about ticket availability, match cancellations, or venue security, causing confusion, panic, and impacting attendance.

To mitigate this, ticketing platforms and the franchise need to invest in:

- ★ **Multi-factor Authentication:** Beyond standard logins, implement MFA that uses varied channels (e.g., push notifications, biometric checks) to confirm identity, especially for high-value transactions or access to critical systems.

- ★ **Digital Forensics and Authentication Tools:** Employ tools that can detect deepfake elements in media and verify the authenticity of digital communications.

- ★ **Strong Communication Protocols:** Establish clear, verified channels for official announcements and transactions, and continuously educate fans on how to identify and report suspicious communications.

- ★ **Supply Chain Verification:** Implement stringent verification processes throughout the ticketing supply chain, ensuring that all partners and vendors adhere to robust security standards.

6. Proactive Data Loss Prevention (DLP) Audit and 3rd Party Supply Chain Risk Assessment

Given the vast amount of sensitive data handled by cricket franchises, a **comprehensive Data Loss Prevention (DLP) audit** is critical. This involves:

- ★ **Data Identification and Classification:** Mapping and classifying all sensitive data (e.g., PII of players and fans, financial records, strategic plans) across all systems (endpoints, networks, cloud).
- ★ **Policy Definition:** Defining clear policies on how sensitive data can be accessed, used, stored, and transmitted.
- ★ **Monitoring and Enforcement:** Implementing DLP solutions to monitor data in motion, data at rest, and data in use, with automated alerts and enforcement actions when policies are violated. This helps prevent accidental or malicious exfiltration of data.

Equally important is a thorough **3rd party supply chain risk assessment**. Cricket franchises rely on a complex ecosystem of partners and vendors: ticketing agencies, merchandise suppliers, broadcasting partners, digital platforms, event management companies, and more. Each of these third parties represents a potential entry point for cyberattacks. The assessment should:

- ★ **Identify Critical Vendors:** Pinpoint vendors who have access to sensitive data, critical systems, or whose compromise could disrupt operations.
- ★ **Assess Vendor Security Posture:** Conduct rigorous due diligence on third-party security controls, certifications (e.g., ISO 27001, SOC 2), and incident response capabilities. This includes security questionnaires, audits, and continuous monitoring of their cyber risk posture.
- ★ **Contractual Obligations:** Ensure that contracts with third parties include explicit cybersecurity clauses, mandating adherence to the franchise's security policies and incident notification protocols.
- ★ **Regular Audits and Reviews:** Periodically audit third-party compliance and test their security measures.
- ★ **Minimizing Ransomware Risk:** By understanding and mitigating vulnerabilities within the supply chain, the franchise can significantly reduce its exposure to ransomware attacks, which often exploit weaknesses in third-party networks to gain initial access to the primary target.

Conclusion

The allure and global nature of The Hundred and IPL Cricket Leagues make them prime targets for increasingly sophisticated cybercriminals. While residential proxies offer attackers an insidious cloak of legitimacy, and AI-augmented deepfakes introduce new vectors of social engineering and fraud, a proactive and holistic cybersecurity strategy can build resilience.

By adopting SASE, integrating cybersecurity with core business objectives, fostering strong C-suite ownership, leveraging expert technology and managed services, and diligently auditing data loss prevention and third-party risks, cricket franchises can protect their digital assets, maintain fan trust, and ensure the uninterrupted thrill of the game for years to come. The future of cricket, like all modern enterprises, depends on a robust defence in the ever-evolving cyber arena.

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.