BLOG REPORT

Protecting the Franchise: Quantifiable Cybersecurity KPIs for the Boardroom.

TIAKI

The digital arena: a battlefield for data and reputation

In the high-stakes world of global sports, where fan loyalty is a currency and digital engagement is paramount, organizations like Manchester United, Real Madrid, the NY Mets, and the San Francisco 49ers face a new, formidable opponent: AI-powered cybercrime.

The sheer scale of their operations, coupled with the treasure trove of fan data they possess, makes them prime targets for sophisticated attacks. To stay ahead of the game, these sporting giants must embrace robust cybersecurity governance, with clear Key Performance Indicators (KPIs) presented regularly to their boards and C-suites.

These organizations are not just sports teams; they are global brands with complex digital ecosystems. Their websites, mobile apps, social media platforms, and e-commerce portals are constantly bombarded with traffic, providing ample opportunities for cybercriminals. The stakes are immense: data breaches can lead to financial losses, reputational damage, and a loss of fan trust. Moreover, the rise of AI-powered attacks has dramatically escalated the threat landscape, demanding a proactive and data-driven approach to cybersecurity.

The AI-augmented cybercriminal has industrialised their value chain

The speed and complexity of the AI-powered data breach attacks towards sports organisations are forecast to increase significantly in 2025.

The eight AI-powered attack tactics outlined below underscore the sophistication of modern cyber threats. Traditional security measures are no longer sufficient to counter these advanced attacks.

1. **AI-Driven Phishing and Social Engineering:** The ability to craft highly personalized and convincing phishing campaigns through AI-driven analysis of social media data makes it incredibly difficult for fans and employees to distinguish between legitimate communications and malicious attempts.
    - **Sports Example:** Imagine an AI-generated email, tailored to a specific season ticket holder, that appears to be from the team's official ticketing system. It claims their account has been flagged for a "loyalty upgrade" and requires immediate login via a link. The email uses the fan's past purchase history, favorite players, and even recent social media posts to make it seem authentic, leading them to a fake login page that steals their credentials.
2. **AI-powered chatbots and Deepfakes:** The ability to extract information and manipulate trust using AI-powered chatbots and deepfakes amplifies the effectiveness of social engineering attacks.
    - **Sports Example:** A deepfake video surfaces online, appearing to show a star player making controversial statements about the team's management or a rival club. This video, disseminated through social media and AI-powered chatbots on fan forums, could trigger widespread fan outrage, damage the player's reputation, and even impact ticket sales or sponsorship deals before the team can debunk it.

3. **Data Poisoning and Model Manipulation:** The corruption of AI models used for fan engagement and marketing can lead to reputational damage and manipulation of fan behavior.
    - **Sports Example:** A team uses AI to personalize marketing emails based on fan preferences. Attackers inject false data into the AI model, causing it to send out emails promoting rival team merchandise or offensive content, leading to a public relations crisis and loss of fan trust. Or, they manipulate the AI that predicts attendance, causing the team to over or under staff events, resulting in financial loss and fan dissatisfaction.
4. **Automated Account Takeover and Credential Theft:** The speed and efficiency of AI-powered credential stealing attacks can compromise a vast number of fan accounts in a short period.
    - **Sports Example:** During a highly anticipated ticket sale, AI-powered bots rapidly attempt to log into thousands of fan accounts using stolen credentials. Successful attacks allow these bots to purchase large quantities of tickets, which are then resold at inflated prices on the secondary market, frustrating genuine fans and damaging the team's relationship with its loyal base.
5. **AI-powered Password Prediction:** The ability to predict common password variations greatly increases the success rate of ‘password guessing’ attacks.
    - **Sports Example:** Attackers use AI to analyze common password patterns among fans, such as using player names, jersey numbers, or team mascots. This allows them to quickly crack a significant number of fan accounts, leading to data breaches and potential financial losses for fans who have stored payment information.
6. **AI-powered Multi-factor Authentication (MFA) Bypass:** The analysis of user behavior related to MFA challenges can allow attackers to bypass this critical security measure.
    - **Sports Example:** An attacker uses AI to analyze the timing and patterns of a team employee's MFA verification requests. They learn when the employee is most likely to approve a request and then launch a simultaneous attack, mimicking the expected behavior and bypassing the MFA security. This allows them to access sensitive internal systems.
7. **API Exploitation and Data Scraping:** The exploitation of API vulnerabilities and the use of AI-powered web scraping tools can lead to unauthorized access to sensitive fan data.
    - **Sports Example:** Attackers exploit a vulnerability in the team's API, which is used to integrate with third-party apps for ticketing and merchandise. They use AI-powered web scraping to extract vast amounts of fan data, including names, addresses, purchase history, and even credit card information, which they then sell on the dark web or use for targeted phishing campaigns.
8. **Advanced Malware and Zero-Day Exploits:** The creation of advanced malware and the exploitation of zero-day vulnerabilities through AI-driven analysis pose a significant threat to the security of club systems.

- **Sports Example:** Attackers create an AI-powered malware that specifically targets the team's point-of-sale systems at the stadium. This malware can evade traditional antivirus software and steal customer payment information during transactions, leading to significant financial losses and reputational damage. Or, they find a zero day exploit in the software the stadium uses to control physical security, and lighting, and use it to cause disruption during a major event.
    i. With weak IoT security or a lack of Network Segmentation in the stadium this becomes a likely point of entry for the cybercriminal who can then move laterally to breach critical systems such as stadium floodlights during a live game or stadium security camera network or point of sales systems.

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

The Governance Playbook:
Building Cybersecurity Resiliency and Effective KPIs for Success

To stay ahead of the AI-powered cybercriminal gangs, sports organisations must rapidly recognise that their threat exposure in 2025 has fundamentally changed. Without investing, prioritising or creating awareness throughout their organisation, it is simply a matter of WHEN not IF they will become victim to a significant cyber attack that threatens their business model.

To put this in context, our team recently held an AI cybersecurity governance meeting with Group Risk at a large European bank. They assess that 70% of medium-sized businesses that become victim to a cyberattack will be bankrupt within 12 months, due their inability to continue effective operations with their customers and partners. Consequently, they do not want a future 'book of business' with corporate clients that have immature cybersecurity operations and now decline corporate customer applications from organisations with lack of buy-in from the C-suite and weak cybersecurity resilience.

The threat can no longer be downplayed or ignored. If you are a C-suite executive reading this blog, our guidance is do not delegate this critically important business function, keep ownership and accountability of your cybersecurity next steps.

Building a Culture of Cybersecurity Resilience

To confidently expand digital business models and accelerate digital monetisation opportunities, sporting organizations must foster a culture of cybersecurity resilience.

This involves:

- ★ **Investing in security awareness training:** Educating employees and fans about the latest cyber threats and best practices.
- ★ **Implementing robust access controls:** Ensuring that only authorized personnel have access to sensitive data.
- ★ **Regularly updating software and systems:** Patching vulnerabilities to prevent exploitation.
- ★ **Conducting regular security assessments:** Identifying and addressing potential weaknesses in the organization's security posture.
- ★ **Establishing a clear incident response plan:** Ensuring that the organization can quickly and effectively respond to security incidents.
- ★ **Collaborating with security experts:** Partnering with cybersecurity firms to leverage their expertise and resources.
- ★ **Implementing AI powered security tools:** Utilizing AI to detect and prevent sophisticated attacks.
- ★ **Business outcome ecosystem partnerships:** seek cybersecurity ecosystem partners that focus on sports business outcomes and drive operational excellence from a business functional perspective, not just a technical outcome.

Establishing Effective Cybersecurity KPIs for Sport

To effectively counter these threats, boards and C-suites must receive regular, data-driven insights into the organization's cybersecurity posture. This can be achieved through a monthly brief containing a set of carefully selected KPIs.

Proposed 15 Cybersecurity KPIs for Monthly Board/C-Suite Briefs:

1. **Phishing Simulation Failure Rate:** This KPI measures the percentage of employees who fall victim to simulated phishing attacks. A decreasing failure rate indicates improved security awareness.

2. **Mean Time to Detect (MTTD) and Mean Time to Respond (MTTR):** These KPIs track the time taken to identify and respond to security incidents. A shorter MTTD and MTTR indicate a more efficient incident response process.

3. **Vulnerability Patching Cadence:** This KPI measures the percentage of critical vulnerabilities patched within a defined timeframe. A high patching cadence reduces the attack surface.

4. **Security Awareness Training Completion Rate:** This KPI tracks the percentage of employees who have completed mandatory security awareness training. A high completion rate indicates a strong security culture.

5. **The Frequency and Severity of Incidents:** This KPI tracks the number and severity of security incidents that have bypassed existing controls. A decreasing frequency and severity indicate improved security controls.

6. **% Sanctioned versus % Unsanctioned Applications:** This KPI measures the % mix of sanctioned and unsanctioned applications being consumed by employees in the work environment.

7. **API Security Posture:** This KPI assesses the security of APIs, including the number of vulnerabilities identified and remediated.

8. **Account Takeover Rate with MFA context:** This KPI tracks the number of compromised accounts where MFA has been deployed. A low account takeover rate indicates effective account security measures.

9. **Malware Detection Rate:** This KPI measures the effectiveness of anti-malware solutions in detecting and blocking malicious software.

10. **Zero-Day Vulnerability Management:** This KPI tracks the organization's ability to identify and mitigate zero-day vulnerabilities.

11. **Security Budget Allocation and ROI:** This KPI tracks the allocation of cybersecurity resources and measures the return on investment in security initiatives.

12. **Third-Party Risk Management Score:** This KPI assesses the security posture of third-party vendors and partners. This is particularly vulnerable in the sports ticketing supply chain ecosystem.

13. **Compliance with Relevant Regulations (e.g., GDPR, CCPA):** This KPI tracks the organization's adherence to relevant data privacy regulations.

14. **AI-Driven Threat Detection Metrics:** This KPI tracks the effectiveness of AI-powered security tools in detecting and preventing AI-driven attacks. This should include metrics on anomaly detection, behavioral analysis, and predictive threat intelligence.

15. **Fan Facing Application Security Testing Results:** This operational KPI tracks the results of security testing done on all fan facing applications, and the speed of remediation of critical issues.

The Final Whistle: Securing the Future of Sports

In the digital age, cybersecurity is no longer a back-office concern; it is a strategic imperative. Boards and C-suite executives at sporting organizations must recognize the evolving threat landscape and prioritize cybersecurity governance.

By fostering a culture of security awareness, implementing robust KPIs and embracing innovative security solutions, these organizations can protect their valuable data, preserve their reputation, and ensure the continued trust of their fans. The scoreboard of security is just as important as the one that reflects game results. To remain at the top of their respective leagues, securing their digital playing field is essential.

About the Authors:

Rob Peters
Global SOC Lead Architect
www.orangecyberdefense.com
rob.peters@orangecyberdefense.com

Orange Cyberdefense

Rob is the Global SOC Lead Architect SASE at Orange Cyberdefense, focusing on Orange's global strategy and offerings for Managed & Co-Managed SASE/SSE services. He works closely with ecosystem partners, industry cybersecurity experts and global SOC operational teams to differentiate vendor agnostic SASE offerings.

By using a business priorities first approach to what has long been seen as a pure technical subject, Rob supports driving the discussion from a strategic level instead of just an operational one. As co-developer of Orange Cyberdefense's Business Objectives he supports customers with clarifying what is required from a business point of view first, before deep diving in what is needed from a technical perspective. This leads to a more proactive and thought leadership driven approach that better supports organizations in implementing the required security controls, in order to have robust protection against malicious actors.

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.