International Journal Research of Leading Publication (IJLRP)
E-ISSN: 2582-8010 ● Website: www.ijlrp.com ● Email: editor@ijlrp.com

Cybersecurity in Sports: Protecting Sensitive Data in Digital Sports Ecosystems

Srinivas Balasubramanian

Abstract

Digital technology has become a cornerstone of modern sports, transforming athlete management, performance tracking, and fan engagement. From wearable sensors that monitor biometrics to AI-driven analytics that enhance game strategies, technology has ushered in a new era of precision and efficiency. However, as sports organizations increasingly rely on digital platforms, they also expose themselves to significant cybersecurity threats.

The rise of interconnected systems, cloud-based data storage, and smart stadium technologies has made sports organizations prime targets for cybercriminals. Sensitive data, including athlete health records, financial transactions, and strategic game plans, must be safeguarded against breaches, unauthorized access, and cyberattacks. Sports entities must not only adopt stringent cybersecurity measures but also stay ahead of evolving threats.

This paper explores the landscape of cybersecurity in sports, examining existing methodologies used to protect digital assets, the challenges sports organizations face in securing their data, and emerging trends in cybersecurity. Additionally, it provides actionable recommendations to strengthen cybersecurity frameworks, ensuring the integrity, confidentiality, and availability of critical information in digital sports ecosystems.

Keywords: Cybersecurity, Sports Technology, Data Protection, Digital Threats, Athlete Privacy, Cyber Risk Management, Secure Sports Ecosystems, AI in Security

Introduction

The growing usage of digital technologies in sports has generated a vast amount of data, from athlete statistics to fan engagement data. While these advancements increase efficiency and the fan experience, they also expose sports organizations to new risks and threats, such as data breaches, phishing scams, and ransomware. With cybercriminals attacking sensitive data, the need for cybersecurity in sports has never been greater. Here, I examine the significance of cybersecurity in digital sports ecosystems and how organizations may deploy preventative measures to preserve data.

Methodology

This paper involves a methodology of qualitative research approach, analyzing case studies, industry reports, and expert insights on cybersecurity in sports. Data is from cybersecurity firms, sports organizations, and academic publications, ensuring a comprehensive understanding of current challenges and best practices in sports cybersecurity.

CaseStudies

- *"Microsoft reported in 2019 on how Russian state hackers attacked the computers of at least 16 national and international sports and anti-doping organizations. Around the same time, the World Anti-Doping Agency (WADA) discovered that failed drug tests of Russian athletes had been erased from a critical data set.*
- *In 2019, a drone with live video feed was used in an attempt at gaining a betting advantage for an in-running horse race bet. In-running or in-play bets allow for betting while a sports game or race is in play and with dynamically changing odds. Live drone footage can be seconds quicker than live TV feeds of the same sporting event, thus providing gamblers with a significant edge. This example demonstrated the shifting landscape of gambling and how technology is providing mechanisms for gaining significant advantage.*
- *In 2019 the Instagram account of Wimbledon champion Simona Halep was hacked and used in an attempt to deceive her 1.3m followers into donating money to fraudsters. • In a 2020 NCSC research survey, at least 70% of sports organizations experienced a cyber incident or breach, with approximately 30% of those incidents causing an average financial damage of £10,000 per incident. The biggest single loss for one sports organization was over £4m.*
- *In 2020, NCSC also reported that the email address of a Premier League club's managing director had been hacked during a transfer negotiation and only intervention from the bank prevented the club from losing around £1m. Additionally, the same report mentioned an English Football League (EFL) club that had fallen victim to a ransomware attack, leaving the club unable to use their corporate email. The club's stadium CCTV and turnstiles were also affected by the ransomware, since they were connected to the same network, rendering them non-operational and almost resulting in a fixture cancellation.*
- *Since 2021, "Project Red Card", led by former Cardiff City manager Russell Slade has been threatening legal action against major gaming, betting and sports data companies over alleged unlawful selling of personal information and performance statistics of players. The project continues to gain support from hundreds of players across football and cricket demanding compensation for the trading of their data in a £500m lawsuit."*

Source – The Hidden Opponent: Cyber Threats in Sport by NCC group & Phoenix Sport & Media Group

Challenges in Cybersecurity for Sports

1. Data Breaches and Athlete Privacy

The sensitive or the biometric data of athletes like hear rate, sleep history, injury details, training plan etc. are stored digitally which will eventually lead to cyber-attacks and threats. Unauthorized access to these sensitive data leads to privacy concerns and it has other disadvantages. Any attack on the wearable technology devices will impact the athlete data.

2. Ransomware and Financial Threats

Sports organizations and high-profile athletes are always one of the major targets by the cybersecurity criminals and ransomware attacks. Unauthorized access to their sensitive data are often leveraged by the

criminals and asked to pay money in place of not releasing those confidential data. Many organizations and sports governing bodies have been a part of these threats.

3. Human errors & Threats

Staff, athletes, coaches and team managers who has access to more confidential data can sometimes become careless or even compromise the cybersecurity. This type of errors can become a major threat and also there are lot of chances in data breach and leakage of sensitive information of the particular individual or the team.

4. Poor Network

Public places, training areas, gyms, stadiums, airports, hotels, social media and other areas and platforms where athletes, staffs, team members and coaches rely on local networks even the poorly secured Wi-Fi connections are vulnerable to cyber-attacks which may lead to data leak.

5. Third-Party Risks

Athletes and sports organizations partner with third party companies for performance tracking, data analytics and fan engagement. Any attack on the third-party company database or network will end in major data breach and leak which will compromise the individual's privacy.

6. Weak security

Fans and spectators are also often target of cyberattacks with respect to the sports. Fans are targeted either with the data that they provide in the third-party websites when they purchase tickets, merchandise etc. These credit card information and the personal details are easy to retrieve if the third-party website or POS is not following a strong protocol in maintaining their servers. It's also easy for the cybersecurity criminals to get their data if they are connected to the stadiums or venue networks during the sport events.

Literature Review

Existing literature highlights the increasing cyber threats in the sports industry and the nature of attacks. Studies show that organizations with proactive cybersecurity strategies, including encryption, multi-factor authentication, and AI-driven threat detection, experience fewer breaches. Researchers emphasize the role of compliance with data protection laws such as General Data Protection Regulation (GDPR) and sports-specific security guidelines to mitigate risks

Future Trends & Recommendations

1. AI & ML for Threat Detection

Artificial Intelligence can be used to detect the threats or any potential cyber attacks based on the data from various sources like phishing emails, network traffic and user behavior. AI can analyze the large and complex pattern of data faster and alert the users at the earliest which will help in mitigating any potential breach.

2. Blockchain for Data Security

Blockchain is another major technology that are currently being used by major car companies and hotels for the keyless entry concept. The Blockchain is known for its encryption, decentralization and immutability which plays a major role in preventing data breach. Using blockchain in sports industry will avoid these potential cyber threats.

3. Cybersecurity Regulations

Sports organizations, third party companies involved in maintain athlete's performance and biometric data along with the governments should implement stronger protocols and regulations to avoid any data breach and data leakage from their system and all wearable technologies that are being used by the athletes.

4. Cybersecurity Awareness and Training

Sports organizations should invest time and money in providing training and create awareness for their team members, staffs, athletes and managers which will be helpful in avoiding any human errors or responding to any malicious emails or clicking any links that they receive posing it to be an official one.

5. Securing IoT and Wearable Devices

Companies focused on the wearable devices and IoT devices should invest more money in developing robust applications that are very difficult to be cracked by cybersecurity criminals or malicious threats. This will help in protecting the sensitive data that are stored in the devices.

6. Implement Multi-Layered Security Measures

Multi-layer security measures like multi factor authentication and implementing stronger protocols and other latest technologies should be implemented to safeguard any critical data that are stored in the applications and other devices.

7. Regular Security Audits and Compliance Checks

Conducting a regular audit and compliance check by the internal team members and also getting an expert opinion from the third-party cybersecurity companies will ensure that we are maintaining stronger protocols and regulations to avoid data breach. It will also tell us if we are on par with GDPR.

8. Disaster and Recovery Management

Preparing a disaster & recovery management plan will ensure that the sports organization or other sports governing bodies are aware of the steps that need to be taken in case of any cyberattacks which will eventually save time and any loss of financial and sensitive data.

9. Enhancing Third-Party Vendor Security Management

Vendors working with sports organizations or athletes should follow the security policies that are coined by those organizations and constant audits should be done to avoid any cyberattacks.

Conclusion

Cybersecurity has become a critical priority for protecting sensitive data, including athlete biometrics, financial transactions, and team strategies. The increasing use of interconnected systems, cloud platforms, and wearable devices has introduced significant risks, making sports organizations prime targets for cyber threats. Addressing these challenges requires a multi-layered security approach, encompassing AI-driven threat detection, blockchain-based data integrity, stringent compliance measures, and ongoing cybersecurity awareness programs.

By implementing robust security frameworks, conducting regular audits, and ensuring strict vendor security compliance, sports organizations can strengthen their defenses against cyberattacks. The integration of emerging technologies such as artificial intelligence and blockchain will further enhance security, providing a proactive approach to threat prevention. Additionally, fostering a cybersecurity-conscious culture among athletes, staff, and management will help mitigate human errors and insider threats.

Moving forward, continued research and collaboration between sports governing bodies, technology providers, and cybersecurity experts will be essential in developing innovative solutions to counter evolving threats. With a proactive security mindset and strong digital defenses, the sports industry can ensure the safety and privacy of its stakeholders while embracing the benefits of technological advancements.

References

1. Halevi, T., & Lewis, J. (2020). "Cybersecurity in Sports: Emerging Threats and Solutions." Journal of Digital Security in Sports, 6(1), 55-72.
2. Johnson, P. (2018). "Third-Party Risks in Sports Data Protection." Cybersecurity Review, 4(2), 101-115.
3. Jones, R., Smith, T., & Brown, L. (2020). "AI-Based Threat Detection in Sports Cybersecurity." International Journal of Sports Tech Security, 7(3), 130-145.
4. Krishnan, S., & Anderson, B. (2019). "The Role of GDPR in Protecting Sports Data." Legal and Regulatory Aspects of Sports Cybersecurity, 5(2), 87-103.
5. Morris, D. (2019). "Blockchain Applications in Sports Data Security." Blockchain and Sports Technology Review, 3(4), 87-102.
6. Paterson, L., & Hanley, R. (2020). "Biometric Data Protection in Sports: Privacy Challenges and Solutions." Journal of Sports Privacy and Security, 5(1), 45-65.
7. Robinson, K., & Kim, H. (2018). "Cybersecurity Training and Awareness for Sports Organizations." Sports IT and Security Journal, 4(3), 90-110.
8. Schatz, D., &Bashroush, R. (2019). "Ransomware Attacks in the Sports Industry." Cyber Risk Journal, 5(2), 77-95.
9. Thompson, J., & White, C. (2021). "Cybersecurity Regulations and Their Impact on Sports Organizations." Sports Law and Security Review, 6(2), 65-80.
10. Woods, P., & Moore, L. (2021). "Insider Threats in Sports Cybersecurity." Journal of Digital Ethics in Sports, 6(4), 120-138.