Cyber threat outlook for the sports industry

By Karen M. Lent, Esq., Anthony J. Dreyer, Esq., and David Simon, Esq., Skadden, Arps, Slate, Meagher & Flom LLP

MAY 15, 2024

The professional sports industry represents the unique intersection of numerous motivating factors for cyber criminals. In recent years, criminal hackers seeking financial gain have hit major sports teams with ransomware attacks. Politically motivated hackers have disrupted live sporting events and leaked player personal data. Foreign governments have even interfered with international sporting events to advance geopolitical aims.

Professional sports teams have seen a meaningful rise in cybersecurity threats over the past decade — an oft-cited 2020 survey from the UK's National Cyber Security Centre (NCSC) found that 70% of sporting organizations are hit by at least one cyberattack annually. Likewise, sports fans have increasingly become the targets of cyber criminals, with a 2023 report (https://bit.ly/3y54gYO) from Lloyds Bank finding that fraudulent football ticket scams on social media had more than doubled versus the previous year.

The sports industry's uniquely multifaceted nature — involving digital and physical events, a wide variety of sensitive customer and player data, and an often international scope — requires that industry organizations stay apprised of a wide array of security threats. Below, we highlight some of the most salient cybersecurity challenges facing the sports industry globally and key legal and cybersecurity best practices to help manage these evolving risks.

Digital transformation

The digital transformation of sporting venues and the spectator experience — increasingly relying on smart devices, online payments, and app-based user experiences — has exposed a wealth of new access points for hackers to penetrate. In early 2019, for example, hackers were able to install credit card skimming malware on the Atlanta Hawks' online store to steal customer payment card information, illustrating the vulnerability of customer payment data to such attacks.

To assist in addressing these concerns, the US Cybersecurity and Infrastructure Security Agency (CISA) and the National Center for Spectator Sports Safety and Security (NCS[4]) have released a publication titled Stadium Spotlight: Connected Devices and Integrated Security Considerations (https://bit.ly/3y7LK1V), which contains a helpful diagram of digital vulnerabilities in a typical sports stadium environment, as well as cybersecurity risk mitigation principles and resources.

Corporate espionage

Professional sports teams also increasingly rely on troves of proprietary data and analytical models to determine their approach to everything from draft picks to in-game strategy.

The digital transformation of sporting venues and the spectator experience — increasingly relying on smart devices, online payments, and app-based user experiences — has exposed a wealth of new access points for hackers to penetrate.

This data presents a valuable target for industry competitors and malicious actors aiming to leverage it for financial gain — as occurred in 2015 when St. Louis Cardinals scouting director Christopher Correa was arrested and prosecuted for hacking into a Houston Astros database that contained confidential scouting reports, trade details, and various other valuable statistics. Correa was later sentenced to 46 months in prison, and the Cardinals were fined $2 million by the MLB and forced to surrender two draft picks to the Astros.

Ransomware threats

Ransomware remains a ubiquitous threat across all industries — and professional sports is no exception. Early last year, the Royal Dutch Football Association (KNVB) reported paying an undisclosed sum in ransom to the prolific LockBit ransomware gang, which potentially stole personal data of over 1.2 million employees and members (https://bit.ly/4dwzXdY).

In previous years, significant ransomware incidents have also impacted the San Francisco 49ers, the Houston Rockets, and the Manchester United Football Club.

Insider threats

In addition to battling external threats, sports industry organizations must also implement internal controls to prevent misuse or theft of data by insiders.

For example, the Italian football club Lazio fell victim to a phishing scam in 2018 that resulted in the transmission of fraudulent wire instructions, which the club used to send £1.75 million that was supposed to be part of a player transfer deal with a Dutch club. Reports (https://bit.ly/3Ut74GK) observed that the hackers likely had insider knowledge of the deal, which they used to perpetrate a man-in-the-middle attack.

Nation-state actors

Some major sporting events and sports organizations have significant international exposure, rendering them prime targets for nation-state actors with geopolitical agendas.

To take one high-profile example: In 2016, hackers purportedly associated with the Russian group "Fancy Bear" targeted the accounts of various World Anti-Doping Agency (WADA) officials via spear-phishing attacks, as reported on the WADA website (https://bit.ly/3WzgLWH). See also, "U.S. Charges Russian GRU Officers with International Hacking and Related Influence and Disinformation Operations," U.S. Dept. of Justice, Oct. 4, 2018. The attack succeeded in leaking medical data pertaining to various Olympic athletes, including information about therapeutic use exemptions for banned substances.

Professional sports organizations should be aware of what data they are sharing with vendors and evaluate the adequacy of their third-party risk management procedures regularly.

The incident was widely seen as politically motivated retaliation for WADA's July 2016 report that called for Russia to be barred from Rio's Summer Olympics due to evidence of organized doping by Russian athletes.

Best practices to manage and mitigate evolving risks

In the face of these challenges, there are a series of widely adopted practices — both technical and legal in nature — that can help organizations across the cyber maturity spectrum diminish their vulnerability to cyber risks. Examples of these best practices recommended by governments and private sector experts alike include:

- **Know what sensitive data your organization maintains and where it is stored.** Professional sports teams maintain a wide variety of sensitive data, including: confidential business data, proprietary draft and trading data, customer personal and financial information, and player medical records. It is important to understand where that data is, what protections guard it, and who has permissions to access it.
- **Know your third-party vendors and what data they receive or have access to.** Third-party vendors and service providers are an increasingly common vector of attack for cybersecurity threat actors. For example, a 2021 attack on the consulting firm Horizon Actuarial Services LLC compromised personal data from the benefits plans of numerous Major League Baseball players and their families. Professional sports organizations should be aware of what data they are sharing with vendors and evaluate the adequacy of their third-party risk management procedures regularly.
- **Implement multi-factor authentication and secure password management policies.** Many cyberattacks originate from poor password management — such as employees reusing passwords or lack of multi-factor authentication. The 2016 corporate espionage incident affecting the Houston Astros, for example, originated from an employee's failure to rotate an old password that was compromised. Widely implementing multi-factor authentication, especially for privileged users, and requiring strong passwords with regular rotation can avoid a number of very common attack patterns.
- **Implement tools to monitor your networks and detect suspicious activity.** Early detection can be the difference between a minor incident and a major event that takes months or years to recover from. Sporting organizations can partner with security firms to continuously monitor network traffic and implement endpoint detection tools to significantly bolster the security and integrity of their networks.
- **Have an up-to-date cyber incident response plan and conduct regular tabletop exercises to test it.** Having employees who are familiar with the current response plan and can act quickly in an emergency is invaluable in mitigating the impact of a fast-moving cybersecurity incident. Conducting annual tabletop exercises keyed to an organization's risk profile — which can help identify gaps in policy, missing expertise, or necessary tooling — is increasingly an integral part of many organizations' cyber risk management programs.
- **Pre-position crisis response vendors to support when needed.** Onboarding a new incident response vendor, whether they are a law firm, a ransomware recovery specialist, or a digital forensics expert, can be a time-consuming distraction in the midst of a crisis. Engaging vendors under privilege in advance can buy precious time at the outset of an incident.

Cybersecurity and legal frameworks for sports teams

The following guidance from institutions in the US and the UK provides principles and a framework for professional sports teams and other sports industry institutions dealing with cybersecurity risks.

- **NIST Cybersecurity Framework 2.0** (https://bit.ly/3wnBBh2): The National Institute of Standards and Technology (NIST) Cybersecurity Framework, last updated in February 2024, provides a common language for critical infrastructure organizations to assess and manage their cybersecurity risk. See also the CISA and US Department of Homeland Security Cybersecurity Framework Implementation Guide (https://bit.

ly/4bpD7Ov) for specific guidance on implementing the NIST Framework in the Commercial Facilities Sector (which includes sports leagues).

- **CISA partnership**: CISA works with sports leagues, teams, stadiums, and other large venues around the country to develop incident response plans and conduct cybersecurity tabletop exercises. CISA conducts over 150 exercises each year across the US with businesses, schools, and other organizations of all sizes to enhance their security and resilience. In September 2023, CISA conducted its 10th annual cybersecurity tabletop exercise (https://bit.ly/3ULfZ7Q) in partnership with the NFL to simulate an attack on Allegiant Stadium during Super Bowl LVII. The four-hour mock exercise included hypothetical impacts from phishing, ransomware, a data breach, and a potential insider threat, along with cascading impacts on physical systems.
- **PCI DSS**: The Payment Card Industry Data Security Standard (PCI DSS) (https://bit.ly/4dsXJan) is a set of security policies that protect credit and payment card data and transactions for the major card brands. The PCI DSS prevents credit card fraud and theft at point of sale systems like the kind found throughout most major sporting venues.
- **NCSC guidance**: The UK National Cyber Security Centre (NCSC) report on The Cyber Threat to Sports Organisations (https://bit.ly/3wnvIR3) contains cyber risk management guidance, in addition to information on industry trends. The NCSC has also created guidance on Cyber Security for Major Events (https://bit.ly/4b1J4Bu) that addresses security at major sporting events and venues.

About the authors



Karen M. Lent (L) is co-head of the sports practice and head of the New York office's antitrust/competition practice at **Skadden, Arps, Slate, Meagher & Flom LLP**. She represents clients in antitrust, sports and other complex litigation matters at both the trial and appellate court levels. She can be reached at karen.lent@skadden.com. **Anthony J. Dreyer** (C) is a partner in the IP litigation department at the firm, concentrating on intellectual property, sports, entertainment and licensing disputes. He co-chairs the firm's sports practice and oversees its trademark and copyright practice. He is based in New York and can be reached at anthony.dreyer@skadden.com. **David Simon** (R) is co-head of the global cybersecurity and data privacy practice at the firm. He helps boards and executive teams navigate rapidly evolving legal compliance issues involving cybersecurity, AI and privacy. He is based in Washington, D.C., and can be reached at david.simon@skadden.com. Joshua Silverstein, cybersecurity and data privacy counsel, and Kyle Kysela, litigation associate, contributed to this article.

This article was first published on Reuters Legal News and Westlaw Today on May 15, 2024.