Sports companies are increasingly the targets of cyber-attacks. Beyond the high costs of third-party liability, first-party risks from cyber business interruption events can temporarily shut down an organization’s operations, causing even more damage to a company and its bottom line.

**WHY SPORTS ORGANIZATIONS?**
A high profile along with possessing vast amounts of sensitive data — including customer, player, and employee information — makes sports companies an attractive target for cyber criminals. Other factors include:

- A lack of cyber awareness, strong controls, and dedicated cyber professionals within sports organizations.
- Competitors looking to illegally access sensitive team data to gain an edge on the playing field.
- The increasing adoption of technology innovations and social media to enhance fan and game experience, has enhanced cyber risks.

---

Data breaches cost organizations on average $7.35 million in 2016.

(Ponemon Institute, 2017 Cost of Data Breach Study – United States, pg. 4)
IN THE NEWS

Recent cyber-attacks against sports companies — including professional sports teams, leagues, venues, fitness organizations, event operators, and others — underscore the evolving nature of cyber-attacks. Those with a thorough understanding of the risks can help make better decisions around insurance and risk management strategies.

**Data Breach:** Data on an unsecured third-party cloud service was leaked, exposing the personal information of three million wrestling fans.

**Ransomware:** The team data of a national car racing association was held for ransom in a cyber-attack. The compromised data was valued at $2 million and estimated to take nearly 1,500 hours of labor to recreate.

**Data Breach:** A national football organization’s union was hacked, compromising the personal data of more than 1,100 current and former players.

**Social Engineering:** A phishing scam against a national basketball team resulted in the release of tax information on all employees to a person impersonating the team’s president.

**Cyber Theft:** A national baseball team official illegally accessed another team’s database to steal confidential player data. The offending team was ordered to pay $2 million and forfeit two 2017 draft picks.

To learn more about cyber risks in the sports industry, contact your Marsh representative or visit [https://www.marsh.com/us/industries/sports.html](https://www.marsh.com/us/industries/sports.html)