



CONVERGING RISKS IN A DIGITAL ECONOMY: SPORTS TEAMS AND LEAGUES

This is one installment in a series of “White Papers” prepared by ThinkRisk Underwriting Agency discussing the converging media and technology risks faced by various industry segments. The White Papers provide real-world examples of these risks, and explore the insurance ramifications of these emerging exposures. This installment of the series discusses risks faced by sports teams, sports leagues and other sports organizations.

Introduction to the convergence phenomenon: Digital technology is a powerful tool that has changed the way businesses and other organizations operate. Digital technology has unleashed corporate creativity, leading to new ways to manage and store data, and new ways to interact and communicate with customers, employees, fans and other constituencies. At the same time, digitization and the way it permits companies to gather, create, distribute and store information and media content has altered the risks of doing business in a fundamental way, and exposes inadequacies in the current insurance response to these new risks. Here’s how this phenomenon affects teams and leagues.

Content: The business of sports has always been about more than presenting games for the purpose of selling tickets and concessions. While the games are the cornerstone of the business model, more and more, leagues and their teams are in the business of engaging the public in many different ways, using all of today’s sophisticated media tools. Examples of these multimedia activities include:

- TV and radio broadcasts (local, regional, national, internet, video-on-demand)
- Publications of all sorts, including magazines, newsletters, media guides and books
- Websites and other social media with both the team’s own content and interactive third-party and user-generated content
- Videos, such as season highlights and instructional videos
- Stadiums and arenas with signage, video displays, music, performances and spectator images

- Designs of logos and mascots
- Original music commissioned by the team or league
- Personal appearances and interviews by owners, management, players and other personalities
- Licensing of logos, player names and images, statistics and other intellectual property rights, as well as merchandising apparel and other goods

Given the extensive array of multimedia activities performed by most sports-related businesses, it is not surprising that there are many examples of media and intellectual property claims involving teams and leagues:

The Baltimore Ravens were sued by an artist who claimed to have given the team the design of their original helmet logo. After extensive litigation, which included a trip to the U.S. Supreme Court, the Ravens were found liable for copyright infringement. After the conclusion of that suit, the artist brought another action over the appearance of the old helmets in promotional and archival footage.

The Seattle Seahawks were sued by Texas A&M University over the Seahawks use of the phrase, “The Twelfth Man,” which A&M has registered as a trademark.

The University of South Carolina and the University of Southern California became embroiled in trademark litigation over the rights to the mark “SC.” South Carolina had used the design “SC” in the 1950s. When the school tried to bring the mark back for use on “throwback” jerseys, Southern Cal, which by then had registered the “SC” mark, brought a challenge. The case went all the way to the U.S. Court of Appeals for the Federal Circuit, which ultimately ruled in 2010 in favor of Southern Cal.

The NCAA co-owned the rights to the trademark, “March Madness,” with another organization. In May 2011, the NCAA announced that it was paying \$17m to settle a dispute regarding rights to the phrase. Given the value of the phrase, the NCAA is extremely aggressive in going after third parties who use the “March Madness” phrase without a license.

Data security and privacy

Digital technology allows organizations like leagues and teams to collect and store vast amounts of data, including employee information but also data concerning fans, customers, vendors and others. This data may include names, addresses, Social Security numbers, personal email addresses, medical information, and of course financial data. In many ways, sports organizations gather data in the same way retail and hospitality companies do, by accepting credit cards for the sale of food, beverages and concessions. Online sales of tickets and merchandise necessarily require the collection of credit card data. In addition, sports clubs reach out to fans to build a stronger community around the teams, often through online communities that involve the collection of personal information. Finally, and unique to sports organizations, the clubs hold financial and medical information about their players, data that is of great interest to the public. Naturally, the breach of that information could be damaging to many parties.

The consequences of a security breach can be significant. In the event of a potential breach of security, state laws in most jurisdictions require the business to notify all potentially impacted persons of the breach, the cost of which can be astronomical. If the information is used in a way that is damaging, the business could face liability claims as well, for failing to protect the data by maintaining reasonable safeguards. In addition, the business may face additional costs such as purchasing credit monitoring services, hiring a forensic team to determine the cause of the breach and take corrective measures, and in some cases hiring a public relations firm to help manage communications with customers and other impacted persons.

The nonprofit organization Privacy Rights Clearinghouse maintains a chronological listing of data breaches, which can be found at www.privacyrights.org. Here are several examples of data breaches that pertain to sports organizations.

In two separate incidents before the 2011 Super Bowl, NFL employees lost laptop computers with unencrypted information about the Super Bowl preparations. Among the data compromised was artwork and security credentials that could be used to create counterfeit passes.

In 2010, it was learned that a database containing the personal details of soccer fans who purchased World Cup tickets through official FIFA-sanctioned outlets had been breached. The data, which included passport details and birth dates of nearly 250,000 fans who attended the World Cup in Germany in 2006, was supposed to have been destroyed after the World Cup, but had erroneously been retained.

In late January 2011, 13 members of the University of Iowa football team were hospitalized after a workout. It was later revealed that the hospital records of the players had been breached.

In April, 2011, the New York Yankees reported that an internal spreadsheet of season ticket holder information was accidentally attached to an email sent to ticket holders.

Coverages in the standard insurance marketplace

Although most sports organizations purchase Commercial General Liability (“CGL”) coverage, typical CGL policies provide limited coverage for media and network security claims. First, the advertising injury provisions in the standard CGL policy contain a broad exclusion for companies that are “in the business of publishing, broadcasting” or other similar media activities. Given the extensive multimedia activities described above, it is quite possible that sports organizations have no advertising injury coverage at all. But even if this broad exclusion were not invoked, coverage under the CGL is quite limited. For instance, intellectual property is excluded, except for copyright infringement in “advertisements,” which is strictly defined. Traditional advertising is only a small sub-set of sports media. This means that the litany of trademark and related intellectual property claims discussed above would likely not be covered. Similarly, website content is generally not covered, unless the content is considered “advertising,” which is construed narrowly. Chat rooms, bulletin boards and other interactive media are excluded. Data breaches and the attendant costs and liabilities are entirely outside the scope of the GCL. Moreover, even when such coverage is provided, it is generally not robust, and the carrier may not have the necessary legal expertise to deal with highly specialized or technical claims.

ThinkRisk's Converging Risk Liability Policy: The Converging Risk Liability Policy from ThinkRisk addresses these unique and emerging exposures, and fills the gaps left by traditional policies. The policy is "modular" and can therefore be customized to meet the needs of the particular sports organization. Coverage Part A of the Policy provides comprehensive coverage for claims arising out of the distribution of content, whether by print, electronic or any other means. To the extent that the organization provides any type of professional service, Coverage Part B provides coverage for claims alleging errors and omissions in the course of providing such services. Coverage Parts C and D provide data security coverage, both for liability claims brought against the organization (Part C) and for certain costs incurred by the organization in responding to a breach (Part D), such as the cost of notifying impacted persons.

To obtain a quote, please contact your insurance agent. For more information, contact us at info@thinkriskins.com or (816) 994-6400.