THE NEXT ARENA OF CYBER EVENTS

Understanding Cybersecurity Risk, Vendor Exposure, and Coverage Gaps in Modern Venues

Up to a few years ago, security at arenas and stadiums mainly consisted of physical gates, bag checks, and crowd management. **Now sports and entertainment venues resemble microcities, technologically built to heighten onsite and external experiences.** From the ubiquitous Wi-Fi to systems that control the lights, video, and HVAC, every part of these venues are linked through digital networks.

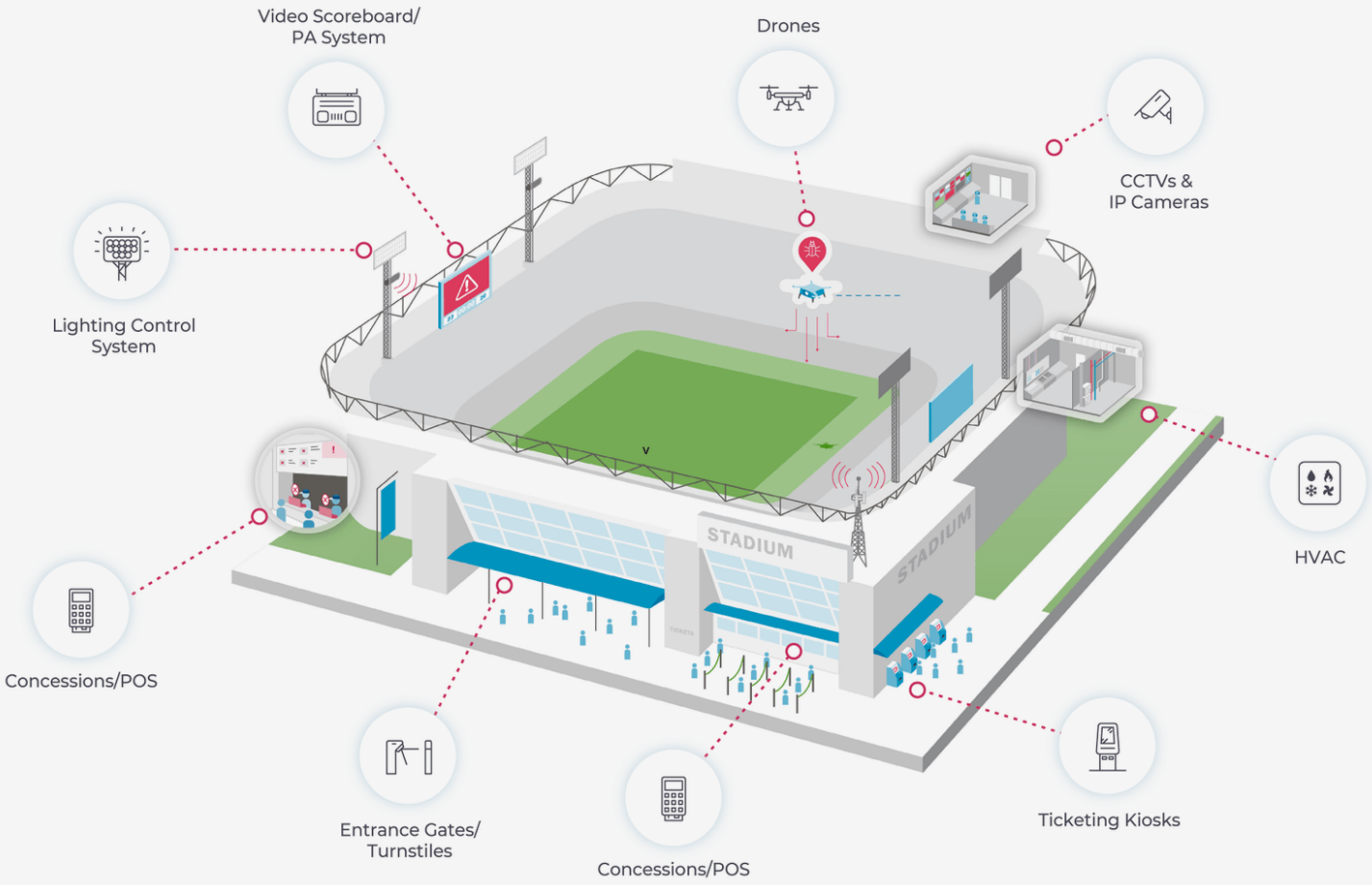
While this interconnectivity helps create incredible live and remote experiences, **it also opens the door to cyber events.** Unlike on-site threats to venues in the past, threat actors don't even need to be in the same country to steal credit card data, disrupt broadcasts, or shut down an event.[1] For venue owners and operators, mitigating these risks is a core part of keeping fans safe and protecting their bottom lines.

THE MODERN ARENA VULNERABILITIES

Cyber events against sports and entertainment industries have escalated over the past several years. These arenas are an attractive, high-profile target, and threat actors are hitting them with a range of cyber events, including ransomware, data breachers, and business interruption.[2] It's not just large arenas in the crosshairs, cyber events have targeted a variety of smaller venues as well, such as zoos, concert halls, and racetracks. **A venue's interdependent network and the public's demand for connectivity and entertainment, underscores the need for robust cybersecurity measures** and risk management strategies for venues of all sizes.

Sports and entertainment venues rely on several networks to create a live, 'smart' experience. This connectivity also provides a large attack surface for bad actors to gain access.

- **Operational Technology (OT):** The systems that run the building, with vulnerabilities such as lighting controls and scoreboards.
- **Fan-Facing Tech:** Public Wi-Fi is always a target. Hackers set up fake Wi-Fi networks (Evil Twin hotspots) that mimic a venue network to steal data or redirect users to malicious websites.
- **Ticketing:** A multi-system vulnerability, ticketing involves third-party vendors and venue management networks. Attackers on ticketing systems have caused significant financial losses, such as the December 2022 attack that shut down the Metropolitan Opera's ticket office, during a season when the venue sells $200,000 of tickets every day.[3]
- **Venue Access:** Attacks that affect egress can create crowd control issues. Denial of entrance can create confusion and delays, while denying exit from an event can create potential panic.
- **Point-of-Sale (POS) Systems:** Onsite sales of food and merchandise are a valuable financial opportunity for venues, teams, artists, and attackers.



Source: OT & IoT Cybersecurity for Stadiums & Arenas. Nozomi Networks.[4]

VENDORS MAY BE A WEAK LINK

Most major events are a complex ecosystem of contractors, sponsors, and third-party vendors. **Research shows that 75% of third-party breaches target the technology supply chain.**[5]

As best as possible, venues should verify all third-party networks are secure, **as a breech in a vendor's system can be used to penetrate a venue's firewalls.** In 2024, a massive data breach at Ticketmaster occurred after an attacker gained access to a cloud database using stolen credentials from a third-party vendor. In this single breach, the attackers claimed to have stolen 1.6 terabytes personal information from 560 million customers, including names, full credit card information, phone numbers, and personal and email addresses.[6]

PROTECTING PHYSICAL RISKS

Cybersecurity should protect more than digital systems connecting data and information, it should also address physical liabilities. The cyber-physical threat is why organizations like CISA categorize stadiums as critical infrastructure. **When a system breach can stop an elevator, turn off HVAC systems, deny egress, an attack becomes a public safety concern.**[7]

During the 2018 Pyeongchang Winter Olympics, malware known as 'Olympic Destroyer' wiped out data on servers right before the opening ceremony. **Attackers not only stole data they also paralyzed the official app, disabled the Wi-Fi, and shut down automated ski lifts.**[8] With several high profile, worldwide events scheduled in 2026, the Pyeongchang attack illustrates why disrupting such events has allure for threat actors.

Third-party attacks are not only targeting technology stacks but also critical infrastructure such as energy grids, HVAC systems, and water supply systems. Unlike an IT breach, in which the object is data theft, an OT breach can lead to real-world, physical damage with devastating public health and safety consequences.[9]

IS TRADITIONAL INSURANCE ENOUGH?

Venue owners and operators may assume their current insurance will cover a cyber event. However, traditional policies often are inadequately able to cover the wide range of risks a venue faces, or, as coverage evolves, policies may be out-of-date. Sports and entertainment venues and organizations require multiple lines of coverage, necessitating careful consideration and evaluation of potential coverage gaps for cybersecurity or data privacy claims.

+ **Commercial General Liability (CGL):** These policies usually only pay out if there is physical property damage or bodily injury. CGL policies are beginning to exclude cyber incidents.
+ **Property Insurance:** Standard business interruption (BI) coverage is often triggered by physical loss (like a fire). If a threat actor attacks a venue's POS systems that shuts merchandise sales, property BI might not cover lost sales.
+ **Biometric Data:** Many stadiums now use facial recognition or fingerprints for entry. In 2024, a class-action lawsuit was filed against the New York Mets, alleging the organization violated biometric data privacy laws.[10] Many cyber policies exclude the unauthorized collection of biometric data, leaving the venue to pay for costs out of pocket.
+ **Crime:** While crime coverage covers financial theft, it often excludes many of the attack vectors associated with cybercrimes. Social engineering may be endorsed, but carriers often cap coverage and limits.

BUILDING A DIGITAL DEFENSE

Cyber protection for venues starts by implementing a proactive, risk mitigation strategy.[11]

+ **Network Segmentation:** Keep guest Wi-Fi separate from operational networks, such as lighting, HVAC, and ticketing. If a threat actor accesses one network, they shouldn't be able to access others.
+ **Rigorous Patch Management:** Maintain constant software release oversight, updating patches and fixing vulnerabilities in every system.
+ **Employee Training:** Staff is the first line of defense. Most ransomware attacks start with a phishing email. Conduct regular training to educate employees to spot scams and report suspicious activity
+ **Incident Response Plans:** Just like plans for a fire or a medical emergency, a cyber event response plan details communication with fans, legal teams, and law enforcement.[12]

THE BOTTOM LINE

In the world of sports and entertainment, the financial costs of a cyber event can be staggering. **Cyber events on sports and entertainment venues can expose personal and venue data, endanger fans' physical safety and venue infrastructure.** Safeguarding venues, organizations, and fans is a critical security concern that requires a proactive and comprehensive risk mitigation strategy.

In today's risk environment, cyber insurance complements cyber controls.[13] Together, they build a defense to protect organizations from cyber events, and a financial backstop for the losses that follow.

[1]Miller, Tim. (2025, September 18). *Most Common Cyber Threats Targeting Major Events*. Dataminr. https://www.dataminr.com/resources/blog/most-common-cyber-threats-targeting-major-events/#:~:text=Large%2C%20crowded%20venues%20like%20sports,how%20organizations%20can%20stay%20ahead.

[2]Liebowitz, Nora G. (2025, May 6). *Game On: Insuring Cybersecurity and Data Privacy in the Arena of Professional Sports*. Saxe, Doernberger, & Vita P.C. https://www.sdvlaw.com/publications/game-on-insuring-cybersecurity-and-data-privacy-in-the-arena-of-professional-sports/#:~:text=Given%20the%20significant%20costs%20associated,coverage%20to%20ensure%20adequate%20protection.

[3]Symphony. (2022, December 12). *As Cyberattack of Website and Box Office Continues, Metropolitan Opera Sells Tickets Through Lincoln Center.* League of American Orchestras. https://symphony.org/as-cyberattack-of-website-and-box-office-continues-metropolitan-opera-sells-tickets-through-lincoln-center/

[4]Nozomi Networks. (n/a). *OT & IoT Cybersecurity for Stadiums & Arenas*. Nozomi Networks. https://www.nozominetworks.com/industries/stadiums-arenas#:~:text=The%20Nozomi%20Networks%20platform%20is,Variety%20and%20Number%20of%20Systems

[5]Avalon, Marie Anne. (2024, February 28). *SecurityScorecard Third-Party Breach Report Reveals Software Supply Chain as Top Target for Ransomware Groups*. SecurityScorecard. https://securityscorecard.com/company/press/global-third-party-risk-report/

[6]Kim, Juliana. (2024, June 1). *Ticketmaster hack may affect more than 500 million customers. NPR*. https://www.npr.org/2024/06/01/nx-s1-4988602/ticketmaster-cyber-attack-million-customers

[7]Miller. (2025, September 18).

[8]Greenberg, Andy. (2019, October 17). *The Untold Story of the 2018 Olympics Cyberattack, the Most Deceptive Hack in History*. WIRED. https://www.wired.com/story/untold-story-2018-olympics-destroyer-cyberattack/

[9]Dataminr. (2025, December 29). *Third-party Vulnerabilities Put the Public Sector at Risk: What to Consider.* Dataminr. https://www.dataminr.com/resources/insight/third-party-vulnerabilities-put-the-public-sector-at-risk-what-to-consider/

[10]Liebowitz, Nora G. (2025, May 6).

[11]IMA. (2025, December 1). *Protecting Organizational Vulnerabilities from Cyber Crime*. IMA. https://imacorp.com/insights/insurance-insights-protecting-organizational-vulnerabilities-from-cyber-crime

[12]Burke, Tim, et. al. (2025, March 10). *Preparing for and Managing a Cyber Attack*. IMA. https://imacorp.com/insights/insurance-insights-preparing-for-and-managing-a-cyber-attack

[13]Burke, Tim, et. al. (2024, October 29). *Protecting Your Organization from Cyber Attacks*. IMA. https://imacorp.com/insights/insurance-insights-protecting-your-organization-from-cyber-attacks