NOW TRENDING IN:
Stadium Security

KEEPING Players and Fans SAFE

To maintain a great experience, venues must secure both physical and network assets.

Photo credits:
juripozzi/AdobeStock
103tnn/AdobeStock
robin/AdobeStock
OSTILL/ThinkStock
Jupiterimages/ThinkStock

On game days, sports arenas and stadiums transform into small cities, with pro hockey and basketball venues hosting upwards of 20,000 attendees, Major League Baseball parks holding 40,000 or more fans and pro and college football stadium capacities approaching or even exceeding 100,000.

These crowds create an electric atmosphere, but they also present security challenges for stadium operators. Rowdy rival fans can often be a source of trouble, but security priorities also include protecting players, limiting access to restricted areas, safeguarding against terrorist strikes and planning for severe weather and natural disasters. In recent years, cybersecurity has risen on this list of priorities, as teams and stadiums send and store more and more sensitive data on their IT networks.

The Need for Venue Security

The 1993 stabbing of tennis star Monica Seles is perhaps the most famous instance of a fan attacking a player, but more than twenty years later, fan-on-the-field incidents continue to occur with alarming regularity. In the spring of 2016, a fan joined players in their on-field celebration after Chicago Cubs pitcher Jake Arrieta threw a no-hitter, and many lower-profile field trespassing incidents happen each year.

In the wake of the Sept. 11 terror attacks, ballparks and stadiums are increasingly seen as a potential "soft target" for terrorists — a fear that was exacerbated by the November 2015 Paris terror attacks, when a terrorist detonated an explosive belt outside the Stade de France after guards denied him entry into a soccer match. Had the blast occurred inside the 80,000-seat stadium, news outlets speculated, it could have caused "unimaginable carnage" and "triggered a manic stampede."

More frequently, fans turn their aggression on one another. A number of teams have struggled to rein in fans determined to engage in violence in stadiums and parking lots. One infamous 2011 incident left a San Francisco Giants fan in a medically induced coma after he was beaten by two fans of the rival Los Angeles Dodgers. Soccer stadiums around the world have been the sites of fan riots that have sometimes culminated in fatalities.

Increasingly, stadium operators are relying on IT solutions to keep fans and players safe. "Technology is very important," says Fred Roberts, director of the Command, Control and Interoperability Center for Advanced Data Analysis at the Department of Homeland Security. "In stadiums, all kinds of systems are now run by computers, including message boards, networked metal detectors and access control for employees, delivery people and even the media."

Lou Marciani, director of the National Center for Spectator Sports Safety and Security at the University of Southern Mississippi, also sees technology playing a growing role in venue security. "You're seeing access control, you're seeing magnetometers at checkpoints for the identification of explosives, you're seeing more sensors down the road," he says. "Biometrics are coming online, particularly in segmented areas of a stadium like media centers, weight rooms and administrative buildings."

Technology solutions are also vital, of course, for cybersecurity efforts at venues, which are not only vulnerable to the same sorts of attacks that affect all organizations, but also often provide network connections for external users such as fans and third-party vendors.

In addition to storing sensitive payment and health data, most teams guard proprietary analytics and player evaluations, which could be worth millions of dollars. The danger of this data being stolen is no longer merely hypothetical. In early 2016, a former scouting director of a Major League Baseball team pleaded guilty to hacking into the player database and email system of a rival team. A U.S. attorney estimated that the hack cost the rival team $1.7 million.

ALL 31 NATIONAL FOOTBALL LEAGUE STADIUMS
will have full walk-through metal detectors in place by 2017.

Source:
SportsBusiness Daily, "How Paris Will Forever Change Event Security," November 2015

Physical Security

Video surveillance has come a long way from grainy black-and-white feeds that had to be monitored by a user in real time. IP-enabled cameras from vendors such as Axis and Cisco not only offer crisp resolution, but also often integrate seamlessly with video management systems that allow security personnel to quickly search through footage in the case of an incident. Some systems, for example, allow users to draw a digital box around an object and then run a search for any movement in that area — a useful tool if, for example,

Best Practice: Know Who Owns the Technology

"Technology can be a force multiplier or a burden, depending upon how it is managed."

That's according to the 2015 Intercollegiate Athletic Safety and Security Best Practices Guide, published by the University of Southern Mississippi and the National Center for Spectator Sports Safety and Security. The guide's authors note that the users of security-focused IT tools such as security cameras and access card readers are often not the personnel responsible for procuring and managing these systems.

Because of this disconnect, the report's authors recommend creating a collaborative team that can "iron out" any issues between different stakeholders, establish who has control over various systems and ensure that all systems operate smoothly during events.

In particular, the report's authors recommend that this collaborative team identify who owns and has budget responsibility for various aspects of IT systems, including purchase and installation, maintenance and service, upgrades and enhancements, and security and hosting.

someone tampers with a precious artifact on display in a team museum.

John Spade, vice president of IT for the Florida Panthers, says the team is looking into cameras with facial recognition capabilities, as well as other biometric recognition systems, to provide access to restricted areas of the arena. "It's a way for players to gain access to the building and practice facilities without having to remember to carry something physical on them," Spade says. "All they have to bring is themselves."

Radio frequency identification (RFID) tags, supplied by vendors such as Zebra Technologies, are another popular method of providing access controls. "We can issue cards that will tell you you're allowed into the stadium, but you're not allowed in the locker room," says Ram Ramaprasad, director of product management for Zebra. "Or you can get a card that says you're allowed into the locker room and the stadium, but you're not allowed into the data center."

The three different types of RFID — low-frequency, high-frequency and ultrahigh-frequency — each have their own distinct advantages, Ramaprasad explains. For example, ID cards utilizing ultrahigh-frequency RFID can be read at greater distances, but that means a security guard is often needed to make sure that unauthorized persons do not attempt to sneak through a door when it opens for an approaching cardholder.

Some event organizers have even begun replacing paper tickets with RFID chips inside wristbands, especially for concerts. These wristbands can be used for cashless payments or to grant special access (such as VIP seating or backstage access), and venue operators can use data generated by the wearables to better understand traffic flows and plan layouts. In 2015, Fast Company questioned whether RFID spelled "the death of the concert ticket."

Technology solutions can also boost overall situational awareness by feeding into a centralized virtual command center, says Marciani. Many teams have implemented software that analyzes multiple data sources, such as video monitoring and access tracking systems, to develop a comprehensive view of a stadium and traffic within it. This situational awareness can help venues improve their decision-making, simplify prioritization and make better use of available resources.

"We can do simulation modeling to make predictions and look at the 'what-ifs,'" Marciani says. "If there's a situation where we have to close Gate 6 because there's an active shooter, what does it mean for crowd management? That's where this is going to."

Information Security

While sports stadiums and entertainment venues face many of the same cybersecurity challenges as other organizations, they also have a unique subset of information security concerns, says Daniel Cole, director of products and solutions at Fortinet.

"In most business environments, traffic variations are fairly minimal,

The Security Balance

Ensuring the physical safety of fans and players is a top priority for stadium operators, but it's not their only priority. They must balance the need for security against the need to provide an excellent fan experience. While travelers have become accustomed to lengthy delays at airport security checkpoints, most fans still expect to be able to enter sports venues relatively quickly, and they may begin to stay home if going to the ballpark becomes as burdensome as business travel.

Recently, some teams have begun rolling out biometric scanners that allow fans to bypass the usual security checkpoints. The San Francisco Giants debuted one solution with a soft launch at AT&T Park in 2014, and the technology has since been used in Yankee Stadium in New York and Coors Field in Denver. Fans can register with the scanning program for free, and then they scan their fingerprints when entering the stadium to verify their identities. Bags are still checked, fans must still present their tickets, and some fans are still randomly screened. But overall, the effect is similar to that of the Transportation Security Administration's precheck program for airports: People get to where they're going faster.

Other teams have tried to reduce wait time to get into the stadium by simply opening more entrance lanes. The Minnesota Vikings added 33 entrance lanes (a nearly 50 percent increase) at TCF Bank Stadium in 2015; two years before that, the Carolina Panthers modified the North and East gates at Bank of America Stadium to allow nearly twice as many fans to be cleared for entry.

100,000

The number of potential cyberthreats discovered on the wireless network at Levi's Stadium in California during Super Bowl 50

Source:
Denver Post, "Denver startup on Super Bowl cybersecurity team found 100,000 threats," March 2016

and administrators have full control of the network devices," Cole says. "Stadiums, on the other hand, have to maintain the logistics and internal network of the stadium data traffic while serving up thousands of concurrent data connections of mobile Wi-Fi traffic to attendees, providing a secure environment while offering Internet service to tens of thousands of 'untrusted' wireless devices."

To prevent stadiums from getting hacked, Coles says, cybersecurity teams should assess the vulnerability of various IT assets and increase security measures for the most susceptible systems. "Having a security fabric approach — including technologies such as enterprise firewalls, wireless security products, specific application security systems and advanced malware platforms — all are critical things to consider when building an end-to-end defense strategy," he says.

But, Cole adds, fan users are actually the most likely target of hackers because their devices collectively represent a potential gold mine of financial data. Hackers might attempt to gain access to credit card data stored on fans' mobile devices by breaking into vulnerable apps, Cole says, or might try to exploit widely used stadium apps by infecting them with malware that later will give the hackers access to individual fans' home or business networks after they download the virus.

To prevent such malicious activity, Cole advises stadium operators to put web application firewalls in place and enforce security filters and firewall policies that prevent wireless devices from communicating with one another directly over the network. Sandboxing and malware inspection systems, Cole adds, can help cybersecurity teams to analyze any files that are being transmitted to and from the network to ensure that the network is not hosting malicious code.

Protecting day-to-day IT systems such as user email is sometimes simpler when these systems are hosted in the cloud, says the Florida Panthers' Spade. "The advantage of increasingly going to the cloud is that I don't have to worry about a denial-of-service attack on my facility," he says.

Until recently, one of the Panthers' biggest cybersecurity nuisances was ransomware, although Spade says that problem has been mitigated by a change in the way the organization performs backups.

Along with sophisticated cybersecurity tools and processes, Spades says, simple user training is important. If a team uses a popular software program to keep track of its player evaluation notes, and users either never change their default passwords or use easily guessed passwords, that can present a huge vulnerability, Spade notes. "I could easily look up the usernames and see all of their notes on players," he says. "It's not so much hacking; it's just people being lazy on passwords."

His own organization isn't immune to the problem. When he first started with the organization, Spade says, one of the most common user passwords was "Panthers."

As in any organization, it can be difficult to get users working inside an arena or stadium to understand the importance of proper cyberhygiene. "I end up doing a lot of evangelizing," Spade says. ■