Sports Innovation Journal, 2024, 20–37
https://doi.org/10.18060/26908

Beyond Gates and Metal Detectors: Understanding Security for Professional Sports Facilities

Steven Watchers, Brian Fowler, and Jimmy Smith

Innovation is of vital importance in professional sport organizations, with various segments and departments catering to diverse managerial functions. While previous research has focused on ticketing, marketing, and event management, the critical aspect of security and intelligence in sports requires further exploration. With the safety of fans, players, coaches, staff, and the local community at stake, security and intelligence play a paramount role. The current research addresses the literature gap pertaining to cybersecurity through in-depth interviews involving 12 participants from major U.S. professional sports leagues and the cybersecurity industry, delving into physical security, personnel security, and cybersecurity domains.

The results of the study highlighted an overall awareness and success in physical and personnel security, but also revealed a concerning deficiency in the understanding of cybersecurity threats. This shortfall emphasizes the pressing need for innovative cybersecurity solutions in the sport industry to ensure the integrity and safety of professional sport organizations in a complex environment. Through such innovative approaches, professional sport organizations can enhance their ability to effectively combat cybersecurity challenges, safeguarding their operations and protecting all stakeholders involved.

Keywords: cybersecurity, personnel security, physical security, professional sport

Steven Watchers, MA, is a graduate from Gonzaga University. His research interests include sports, security, safety, cybersecurity, and risk management. Email: swatchers@zagmail.gonzaga.edu

Brian Fowler, PhD, is a clinical assistant professor in the Department of Movement Sciences at the University of Idaho. His research interests include revenue generation and organizational management. Email: bfowler@uidaho.edu

Jimmy Smith, PhD, is an associate professor in the Department of Kinesiology and Sport Management at Gonzaga University. His research interests include intercollegiate athletics, organizational behavior and sports outreach. Email: smithj1@gonzaga.edu

Introduction

The connection between competitive sports and the notion of national security cannot be overlooked, and organizations hosting these large-scale events must carefully consider security. The 1972 Munich Olympic Games, the 1996 Atlanta Olympic Games, the 2009 attack on the Sri Lanka national cricket team, the 2013 Boston Marathon bombings, and the 2017 Manchester Arena bombing are examples of sporting events targeted to cause physical, psychological, and emotional pain (Jayawardhana, 2016). Considering how to successfully prevent and respond to violent crimes at large-scale sporting events is even more important considering the anti-terrorism climate (Xu, 2018).

The primary focus of current research lies in the realm of cybersecurity innovation in the context of professional sport, given the evident connection between competitive sports and national security concerns. Sporting events have historically been targeted in the physical domain, highlighting the importance of successful prevention and response in the present anti-terrorism climate (Jayawardhana, 2016; Xu, 2018). The general audience associates security measures at sporting venues with an abundance of personnel, metal detectors, clear bag policies, and police presence (National Center for Spectator Sports Safety and Security, 2021). However, security encompasses multiple facets, including physical, personnel, and cyber, where deterring potential attacks becomes essential (Smith et al., 2017).

Professional sport organizations collaborate with law enforcement agencies, and various entities, to publish resources and best practices for securing major sporting events (Federal Bureau of Investigation, 2018; Transportation Security Administration, 2019; United States Secret Service, 2020). However, information and intelligence sharing, particularly in the cyber domain, remain understudied in professional leagues (Shein, 2021). Thus, the innovative nature of the current research aims to demonstrate how improved information sharing equips sport organizations to prevent attacks on their infrastructure.

Given the rapidly evolving advancements in security technology and cybersecurity, continuous research is essential to ensure that sports security keeps pace. The study aims to establish best practices, recommendations, and procedures for a more holistic approach to addressing security threats. The research question guiding the current study is: How can the security of a professional sports facility be improved in the physical, personnel, and cybersecurity domain?

Literature Review

Sports facilities managers must consider security threats as part of their risk management process. Regardless of size and setting, sporting events have a

symbolic significance for millions of people across the globe. "Indeed, it is their social, cultural, political, and economic importance that makes them a potential target for terrorism and has resulted in the implantation of risk management strategies seeking to address this threat" (Cleland, 2019, p. 144). The most common referenced starting point regarding security in sports is the 1972 Munich Olympic Games attack when Palestinian terrorists kidnapped and murdered 11 Israeli Olympic athletes.

> This literature often locates the terrorist attack at the 1972 Olympic Games in Munich as a starting point for the relationship between sport and terrorism before dissecting the impact of the terrorist attacks across the United States (US) on September 11, 2001 (9/11), had on risk management strategies surrounding future elite sport events. (Cleland, 2019, p. 144)

As threats continue to evolve, sports facility managers must keep pace with the risks. Since 2017, the National Basketball Association (NBA), National Football League (NFL), and Major League Baseball (MLB) have taken aggressive measures to improve and reinforce stadium and arena security. Evidence of heightened security is captured by Dyer and Cussen (2019), who state that "Evolving security threats have forced facility owners, operators, and tenants to reassess the security of sports venues" (p. 36). This has led to security costs increasing for mega events such as the Olympics.

Cybersecurity

Sports facilities are increasingly dependent on technology, allowing attack vectors for malicious cyber actors (Cleland, 2019). According to Martin and Robertson (2020),

> Like most of the UK economy, sport is reliant on digital technology. Sport is played in large venues with networked security systems controlling essential functions such as turnstiles and security cameras. Organizations hold a significant amount of sensitive personal data and process millions of financial transactions. (p. 6).

Various tactics, techniques, and procedures (TTPs) used by malicious cyber actors can be utilized against a sports facility, which could incapacitate the ability to function.

Research by Grow and Shackelford (2020) explain that academic research literature up to that point had entirely ignored the sector (cybersecurity) and failed to assess the risks to high-profile leagues and teams. Their article explained how the MLB, NFL, NBA, and National Hockey League (NHL) confront several possible competition-related cybersecurity threats and evaluated the leagues' current security measures (Grow & Shackelford, 2020).

Table 1. Cyberattack Events

Year	Event
1980s	Olympics extensively adopt computer usage for operations, raising concerns about the potential for cyberattacks (Duckworth & Krieger, 2021).
1990	The advent and use of the World Wide Web, the first web browser, enabled access to the internet from a variety of devices and operating systems. It enabled users with limited technological expertise to effortlessly navigate and access various websites.
2015	St. Louis Cardinals investigated for hacking Houston Astros' database (Schmidt, 2015).
2017	Greenwald discusses that the most damaging hacks often exploit correctable vulnerabilities. In September, WADA experiences a spear phishing attack, compromising private medical information of 41 Olympic athletes (Greenwald, 2017).
2021	Darktrace releases a threat report highlighting SaaS, phishing emails, server-side attacks, and ransomware as major cyber threats (DarkTrace, 2021).
2022	CISA and NCS4 collaborate to create "Stadium Spotlight," a product providing an overview of stadium vulnerabilities, risks, and mitigation recommendations (Cybersecurity & Infrastructure Security Agency, 2022).

Duckworth and Krieger (2021) discussed the extensive use of computers by the Olympics to assist in operations since the 1980s and how it posed the possibility of a cyberattack. In addition to boosting security measures, the rising usage of computers has generated a new security factor for event organizers. Keeping a hacker from obtaining unauthorized access to information or disabling power infrastructure is a distinct challenge requiring an innovative solution (Duckworth & Krieger, 2021). Table 1 gives a brief evolution of cybersecurity over the decades.

Cybersecurity professionals at sports facilities are challenged at every event; with minimal investment, a malicious actor can obtain a Wi-Fi mimicking device to create a rogue access point, posing a "man-in-the-middle" threat. Exploiting this vulnerability allows them to intercept financial and personal data transmitted over the Wi-Fi. Operating with just a phone in a backpack, bad actors gain complete control over a venue's Wi-Fi, including stadiums (CISA, 2022). This same device can be repurposed for a denial-of-service (DoS) attack, disrupting network access, leading to revenue loss, and eroding trust. Cyber risks extend beyond commercial motives, with political actors leveraging public platforms like jumbotron screens, as seen in the 2015 ISIS sympathizer hack of Ohio's Eldora Speedway website (Birns et al., 2016).

Physical Security

Sports facilities in the US are critical infrastructure and considered essential resource sectors. According to Hall et al. (2011), critical assets are individual targets whose destruction might cause a local catastrophe and harm the nation's morale. Physical security features may include fences, walls, landscaping, topography, vehicle obstacles, and blast or ballistic protective elements (Dyer & Cussen, 2019). Technical security features supporting physical security include cameras, facial recognition, intrusion detection systems, electronic and mechanical access control points, and screening devices. Similarly, operational security measures include employee training, bag check regulations, facility codes of patron's behavior, bomb detection, and drug screening (Dyer & Cussen, 2019).

Dyer and Cussen (2019) outlined proactive security measures adopted by the NBA, NFL, and MLB emphasizing hostile vehicle mitigation, pedestrian screening, and diverse threat assessments. They proposed a four-step model (detect, deter, deny, and delay) applicable to all facilities. Highlighting the critical role of facility perimeters, the model aims to safeguard organizations. Unmanned drones, while beneficial, pose security risks in sports stadiums, offering surveillance and potential harm. The ease of deploying drones raises concerns about privacy infringement and event safety. Stadium management must deploy robust countermeasures to address the evolving drone threat, ensuring spectator safety remains a priority (Sky Safe, 2023). In 2021, the MLB faced unauthorized drone issues, leading to the suspension of a Minnesota-Pittsburgh game (Crumley, 2022).

Emerging technology can also assist the security apparatus in managing security threats on site. If used correctly, distinct types of video feeds, video analytics, geofencing, and sensors can assist a security element to better protect a sports facility from an attack (Dyer & Cussen, 2019). In 2021, the NCS conducted a survey on sport spectator safety, which revealed that 73.2% of participants consider safety measures when attending an event and 77% want those safety measures visible. The survey provided seven industry recommendations that included the venue/event website, email, and tickets should inform viewers of safety and security precautions, reassure spectators, and use visible security measures like law enforcement and screening technologies.

NCS4's survey on technology usage identified common tools like CCTV, walk-through metal detectors, electronic tickets, fixed bollards, bomb detection canines, and venue signage (NCS4, 2022). Utilizing these technologies is crucial in reducing physical risks at stadium venues.

Personnel Security

It is the duty of the facility owner to balance spectator safety without undue restriction (Tavella, 2010). Hall (2010) highlighted the role of the security force

in ensuring the safe conduct of patrons, emphasizing intelligence sharing for effective personnel security. The security force, consisting of police officers and/or security guards, ensures the orderly conduct of patrons at sporting events (Hall, 2010). Venue leadership must stay informed for timely decisions, and effective intelligence sharing is vital to personnel security, reducing the risk of disorder, injuries, or deaths (Hall, 2010).

Between private and public partnerships, sports facility managers protect their fans, players, coaches, staff, and vendors with law enforcement (Department of Homeland Security Center of Excellence, 2013). The DHS Center of Excellence (2013) identified that sports facility managers should establish security partnerships, protecting fans, players, and staff with law enforcement (DHS Center of Excellence, 2013).

In 2015, during a coordinated terrorist attack in Paris, one target location was outside France's national stadium (DNI, 2016). Following the attack, the NFL released a statement on collaboration with law enforcement, demonstrating awareness of security threats and to enhance personnel security:

> The NFL and team security departments work closely with stadium operation personnel and federal, state, and local law enforcement to provide a safe experience for the more than 17 million fans annually attending NFL games. The NFL and its teams continually evaluate and improve our comprehensive security plan. (Popper, 2015)

Insider threats, as highlighted by Proof Point (2022), involve trusted members abusing authorized access to harm a company's information or systems, and they can extend beyond employees to include third-party vendors, contractors, and partners. These threats may manifest as accidental or deliberate actions, depending on the individual's goal (Proof Point, 2022).

Clear Lines of Effort

Fan experience and revenue generation are two of the most critical aspects of professional sports. Sports facility managers must know, understand, and accept the risks concerning their facilities' cybersecurity, physical security, and personnel security (Cleland, 2019). Facility managers can make better-informed decisions that will be accepted and understood by the executives of the facilities and organizations participating at the venues (Veselinović et al., 2020).

The importance of effective and efficient information and intelligence sharing is evident; however, proper methods and structure to ensure these steps occur may not be as easy. Finding the best practices, providing a baseline standard, proper training, and ensuring efficient risk mitigation plans are prepared is crucial to preventing a complex attack targeting sports facilities. With a better understanding of the methodologies and experiences of sports facility managers

regarding security, practitioners could construct successful and all-encompassing security plans through efficient and effective management.

Methods

To better understand security in professional sport, the current research employed a qualitative investigation into threats sports facility managers face. Security was addressed in sport utilizing three facets: physical, personnel, and cybersecurity.

Due to the lack of research in security—specifically cybersecurity in professional sports—a qualitative grounded theory approach was utilized. Grounded theory allows the researcher to design techniques, data collecting, analysis, and conceptualizing qualitative data (Creswell & Poth, 2018; Crotty, 1998). Grounded theory helps answer questions about process, or how something changes through time (Merriam & Tisdell, 2016). The grounded theory permits the theory to arise from the data before data gathering (Tie et al., 2019). Thus, the grounded theory approach allowed the researchers to apply the data to continue to develop a further understanding of professional sport physical, personnel, and cybersecurity (Creswell & Poth, 2018; Jones, 2015).

Researcher Positionality

In qualitative research, it is important to clarify the underlying philosophical assumptions that directed the development of the research questions and framework so that the reader may better understand the epistemological viewpoint (Creswell & Poth, 2018). Additional justifications should also be made for choices concerning the methodology and procedures of the research (Crotty, 1998). The approach allowed the participants (security personnel) to construct the meaning of the situation (Creswell & Poth, 2018), and the researcher to then interpret those meanings in the context of the research.

All members of the research team have ties to sport; experiences include extensive work in security and intelligence for the U.S. Army, being former NCAA student-athletes, playing professional athletics, and extensive work in collegiate and professional athletics as coaches and administrators. These experiences shaped the research team's view that all types of security are important to sports venue management, and certain areas of security (e.g., cybersecurity) may be overlooked and less understood by venue management. This view then led to the identification and focus of the current research on understanding security in professional sport.

Participants

The participants in the study were obtained through snowball sampling. Snowball sampling entails selecting volunteers who fit the established requirements for

research participation. Once interviews are completed, a request is made to the interviewee for additional recommendations of interview participants. By asking personnel in the field who else to speak with, the snowball grows as more information-rich instances are accumulated (Merriam & Tisdell, 2016).

Procedures – Sampling and Interview Questions

Data collection occurred until data saturation was achieved. Merriam and Tisdell (2016) explain data saturation occurs, "When continued data collection produces no new information or insights into the phenomenon you are studying" (p. 199). Through a previous research proposal and discussions with experts in the fields of sports and cybersecurity, the researcher developed intensive introducing questions. "Such opening questions may yield spontaneous, rich, descriptions where the subjects themselves provide what they experience as the main dimensions of the phenomena investigated" (Kvale, 1996, p. 133). The interview questions pointed at the three aspects of information and intelligence (physical, personnel, and cybersecurity) for research, with the target audience being key security leaders for professional sport organizations and cybersecurity experts.

For the semi-structured interviews, preliminary questions functioned as conversation starters. Sample questions for the interview included: (a) Who is most responsible for gathering and sharing information and intelligence about the security of sports facilities? (b) What do you foresee as the greatest cybersecurity threat to a professional or collegiate sport organization and why? (c) What do you foresee as the greatest physical security threat to a professional sport organization and why? (d) What do you foresee as the greatest personnel security threat to a professional sport organization and why? (e) How can the security of a professional sports facility be improved in the physical, personnel, or cybersecurity?

Analysis

The data analysis process began with the review and categorization of the data collected from the participants interviewed. This included team security personnel and cybersecurity professionals. A data-driven coding technique that refrained from imposing any pre-existing coding framework aligned with the methodology proposed by Braun and Clarke (2006) in which themes emerged naturally, encompassing an evaluation of whether distinct concepts were covered throughout interviews. Subsequently, the findings were structured according to the frequency of cited themes. Next, the researcher identified themes and patterns of the data post-interviews to correctly categorize the information based on words, phrases, and missing information.

"A theme is, essentially, a conceptual label for a group of linked codes, and is more abstract in nature" (Jones, 2015, p. 277). A theme was generated when

eight of 12 participants offered detailed comments related to a topic (i.e., human) in which a theme was then created. The findings added to the main themes by extensively examining the patterns. Lastly, the final analysis and summarization of the data will present the research results.

Results

Participant Demographic Information

There were 12 interviews conducted during this research and participants were affiliated with the following leagues or industries: Federal Cybersecurity Industry (4), MLB (2), Major League Soccer (MLS; 1), NBA (1), NFL (3), and Professional Sports Research Industry (1). All 12 participants in this study were male. Participants have been in their respective positions in their fields between 9 and 34 years. The participants' ages ranged from 34 to 57. The interviews, which lasted 45 – 75 minutes, consisted of semi-structured, audio/video-recorded interviews about each participant's viewpoint and understanding of security threats that sports facility managers face.

Themes

Six themes were identified based on the responses from the 12 participants during the research. Regarding cybersecurity, the themes were "humans" who utilize the networks, cybersecurity does not fall into the traditional security planning process, and lack of knowledge and understanding of cybersecurity threats. Regarding physical and personnel security, the themes were local law enforcement, contracted security staff, and lack of standardized security structure. The themes identified are displayed in Table 2.

Cybersecurity

One of the largest threats and primary themes identified in cybersecurity in any organization is the humans who utilize the network. Source #2 stated, "So, I would say the human is the absolute number one problem. Right. and we don't have the security awareness."

Cybersecurity does not typically fall under the purview of the sports facility manager or security department. It usually falls under the Information Technology (IT) department. Three of the interviewed participants (25%) were cybersecurity professionals, and nine of the participants (75%) were from sports major leagues. Of the 12 interviewed participants, 10 participants (85%) stated they know and understand cybersecurity is critical to a professional sport organization or sports facility; however, only 33% understood cybersecurity's complexity and stated it

Table 2. Themes

Domain	Theme	Participant Quote
Cybersecurity	Humans	So, I would say the human is the absolute number one problem. Right. and we don't have the security awareness. People are easily susceptible to social engineering, through different types of cyberattacks, people are the biggest and softest targets.
	Cybersecurity does not fall into traditional security planning	As facility managers, cybersecurity does not fall into our traditional planning process, like physical or personnel security. We rely on the IT department for that. Cybersecurity is not a responsibility of our facility security team. That is left up to the IT folks.
	Lack of knowledge and understanding of cybersecurity threats	I couldn't begin to tell you what the cybersecurity threats to my facility are. We do not get briefed on cybersecurity threats, that is not our lane. We are briefed only if it is linked to an individual that may attempt to attend the game and we should be on the lookout for.
Physical & Personnel Security	Law enforcement	Just like most other teams in the league, we rely heavily on the police for their presence, K9 support, and assistance in the operations center. I was told they were having trouble recruiting and keeping officers because of the current climate towards cops.
	Contracted security staff	Our organization, like many others, contract out a large portion of our security staff. Most professional sports organizations rely on temporary contracted security staff during season. During the offseason, most teams drop down to minimal security staff.
	Lack of standardized security structure	The league headquarters does not recommend what any of the teams' security structures should consist of. I wish they would provide a standard for all teams. Having worked in a couple professional league headquarters, it was astonishing to see the lack of policies regarding standards for the leagues. The leagues leave it up to the teams and recommendations from law enforcement, but there should be standards applied to establish a foundation.

should be part of the overall security plan. Source #8 said, "As facility managers, cybersecurity does not fall into our traditional planning process, like physical or personnel security. We rely on the IT department for that." Seventy-two percent of facility managers interviewed could not describe the cybersecurity threats their facilities face. Source #1 stated, "I couldn't begin to tell you what cybersecurity threats to my facility are."

Many professional sport organizations utilize technology to monitor their players' health data. All this critical player biometric data can be stored on local devices or a team-controlled server. However, if malicious cyber actors gain access through a vulnerability, they can easily export the data and conduct an attack, such as a ransomware attack. Source #11 stated, "Ransomware is a substantial concern for professional sports organizations. Look at the San Francisco 49ers, who were hit with it in 2022. It wasn't the first ransomware attack of a professional team, and it will not be the last." Source #6 stated, "I would be concerned by ransomware or ransomware affecting them and even organizations that are tied to them."

Source #6 discussed a hacker's different approaches to penetrating a network. "Every database, server, and IT system possesses ways to gain access without being detected. A mid-level experienced hacker could gain access utilizing different toolsets that can be created or purchased for little money. The hacker could grab a chunk of data and exfiltrate the information, or they could leave a tool that intermittently passes data back to the hacker."

Due to the complexity of cybersecurity and prioritizing efforts to identify, protect, detect, respond, and recover from an incident, the organizations cannot protect everything with 100% success. Source #2 stated, "A cybersecurity expert is going to apply resources where things are most important; however, that leaves gaps in other places. It (the network) can't be protected 100% of the time." Assumption of risk is critical to properly defending an organization's network, and the organization must prioritize and divert resources based on priority.

Physical Security and Personnel Security

It was found that nine participants (75%) stated their personnel security plan overlapped with their physical security plan. Two participants (17%) also stated they create a separate personnel security plan for key personnel that will arrive at the facility. All (100%) interviewed participants agreed physical security is one of the most important and complex aspects of securing a professional sports facility.

Source #4 discussed how security looks differently at each facility. "Physical security is the approach organizations and facilities take to ensure the safety of all personnel stepping foot on facility grounds. Security could look different depending on which facility or arena you go to." During interviews with two

separate professional sport organization security managers, they both stated insider threat is a high personnel security concern. Source #1 discussed their concern about insider threats. “I think it’s more of an insider threat because, you know, it’s different times now. I, I think with the economic situation, you know, when an employee gets laid off or let go, you know, especially when it’s an employee that had access to so much information or, or knowing kind of like the facility and things like that, you know, there, there’s always that concern of them trying to come back and doing something malicious.” Insider threats and workplace violence need to be possibilities that sports facility and venue management personnel consider. Source #10 stated,

> Insider threats coming from current and past employees is a major concern for the sports industry. During the pandemic, a lot of people in sports, including professional sports lost their job, took a pay cut, or were forced to acquire more responsibilities they were not originally hired or trained for. They are overworked and tasked, however, those people are scared to say anything due to fear of losing their job.

Source eig#8 specifically discussed how active shooters are a threat to all patrons in the immediate area; however, the second-order effect of an active shooter situation is panic among other fans/patrons. Sports facilities have large parking lots/structures. An active shooter scenario in a professional sports facility parking lot would be difficult to deal with due to vehicles, open space, panicking fans, and reaction time from security. Subject #1 specifically commented as follows:

> An active shooter is probably one of the greatest threats. It’s up there because we have a big parking lot, so having some type of active shooter scenario out there, it can happen. And our stadiums are surrounded by gates. But if something happens in the parking lot, that’s going to create great panic inside. And at that point, once the shooting starts outside the gates, no one’s going to be able to stop somebody from coming to the gate after they’ve been fired upon. Especially when there are thousands of fans in the immediate area.

Sports facility managers, team owners, and leagues rely on local, state, and federal law enforcement to provide a police presence at sports facilities. Source #3 stated the relationship between sports facilities and law enforcement is critical for security. “Law enforcement support in conjunction with venue security staff is critical for the safety and security of the venue. Without the assistance of local, state, and federal law enforcement, the venue could not be properly secured.”

Police department shortage is influencing the department’s ability to assist sport organizations. If this trend continues nationwide, law enforcement’s ability to support sports venues will be impacted. Source #4 stated:

> With the current police shortage issues in some major cities, law enforcement support to the sports industry will be impacted. Not only will the shortage have an effect, but the quality of new recruits due to loosening standards will have an effect as well. Smaller police departments with limited training, resources, and experience will be relied on more to fill the gap at sports venues, possibly affecting the overall security posture.

Professional sports facility managers rely on local law enforcement to provide security and support. Without law enforcement support, it would be difficult for professional sports to provide the level of oversight needed to enhance the security posture. Source #4 also stated, "Just like most other teams in the league, we rely heavily on the police for their presence, K9 support, and assistance in the operations center."

Source #9 discussed other physical and personnel security concerns that facility managers face are fans running onto the field or court during a game, threatening officials and players, fights between fans, workplace violence, and insider threats. Although some of these cannot be avoided without jeopardizing the fan experience, such as fans running onto the field or court, threatening officials and players, and fights between fans, others need to be looked at more closely.

Organizational Security Structure

There is no standard format for professional sport organizations' security structures. Professional leagues, teams, and facilities have diverse ways of approaching their organizational security structure. Source #5 stated, "Budgets, the organizations' size, location, and resources play a large role in how security is treated throughout different leagues."

Sport organizations rely on local, state, and federal law enforcement to assist with facility management security at sports facilities. Source #7 stated, "And today at every game, there is law enforcement, whether it's local, state, or federal, who directly support the venue ensuring safety and security are handled."

Discussion

The current research effort sought to understand and identify security threats sports facility managers face regarding cybersecurity, physical security, and personnel security. The findings would aid sports facility administrators in improving their capacity to manage, secure, and protect their facilities. Seven sports facility and security managers, four federal cybersecurity industry professionals, and one professional sport research organization were interviewed regarding concepts discussed by experts in the fields of cybersecurity, physical security, and personnel security of sport management to achieve the objectives of the current study.

Professional sport organizations have developed their own internal, proprietary information systems to aid in personnel and strategic decision-making. These databases are a potential goldmine of information, including most of a team's current internal thought processes.

Overview of Key Findings

The current study sheds light on varied experiences and a lack of standardization in physical and personnel security knowledge within sports facility management. Recognizing gaps in cybersecurity and holistic security approaches, this calls for innovation and improvement in cyber resilience in several ways.

1. **Security Knowledge Gaps:** The study reveals disparities in physical and personnel security knowledge due to non-standardized factors. Recognizing these gaps can empower sports facility managers to enhance security posture by addressing knowledge weaknesses and leveraging available security, information, and intelligence resources.
2. **Cybersecurity Challenges:** Sports venues heavily rely on connected digital devices, posing potential cybersecurity risks. Despite 87.5% having a cybersecurity defense program, the increasing reliance on connected devices requires constant innovation. A single breach could jeopardize critical systems, urging the need for enhanced cyber resilience (Cybersecurity & Infrastructure Security Agency, 2022; NCS4, 2022).
3. **Digitization in Professional Sports:** Professional sports leagues, especially the NFL, face cybersecurity challenges with the digitization of team workplaces. The reliance on tablets introduces threats, emphasizing the necessity for improved cybersecurity measures. Emerging technologies monitoring players' metrics also pose potential risks that require innovative solutions (Grow & Shackelford, 2020).
4. **Planning and Knowledge Gap:** Planning is identified as essential, yet a knowledge gap exists in cybersecurity aspects during security planning. Facility managers often overlook cybersecurity threats in the planning process. Closing this gap by integrating cybersecurity considerations can enhance the effectiveness of security measures at sports facilities (Duckworth & Krieger, 2021; Veselinovic et al., 2020).
5. **Reliance on Third-Party Security Staff:** The study indicates that 71% of facility managers rely on contracted security staff, posing challenges in ensuring the quality and experience of the contracted company. While cost-effective, it highlights the need for innovative solutions to address potential shortfalls and ensure optimal security support (NCS4, 2022).

6. **Technology Advancements:** Technology plays a crucial role in assisting sports facility managers. Innovations like video analytics and millimeter-wave technology offer advanced security solutions. Integrating such technological advancements is essential for effective threat detection and response in sports venues (Subject #11).
7. **Standardized Security Structure:** The absence of a standardized security structure for sports facility managers emphasizes the need for innovative solutions. Organizational structures recommended by leagues and partnerships like InfraGard offer valuable support, enhancing education, information exchange, and training on emerging threats (FBI, 2018).

Limitations and Future Research

Representing various organizations, from professional sports to Federal Cybersecurity Professionals, the research emphasizes collaboration in ensuring the safety of all stakeholders. Sharing information across leagues and federal agencies provides a holistic view of cybersecurity in professional sports. Future research could narrow the focus to a single professional association, delving into its cybersecurity philosophy.

While risk management was lightly discussed in 25% of interviews, with its importance acknowledged, no specific questions were established during the research planning phase. Future studies should delve deeper into risk management with facility managers, teams, and leagues, as it plays a crucial role in security planning. Budgets significantly impact staffing, resourcing, and equipment in non-revenue-producing sections like security and intelligence in the sport industry. Future research should further explore funding dynamics, establishing a baseline, sharing lessons learned, and determining the cost balance needed to adequately support security and intelligence requirements for facility managers.

Conclusion

Sports facility managers are responsible for many factors to ensure their facilities' proper operation and function. They work with and coordinate with other teams in the facilities to ensure successful operations. Against potential risks, sports facility managers and event organizers have implemented new technical equipment, enacted new regulations, and established operations centers.

This study sought to identify the many security threats faced by facility managers. This study revealed a correlation between growing dangers and the challenges faced by facility managers. Sports facility managers rely on their security section to handle and prepare for all scenarios threatening the facility, players, and fans. A holistic view of cybersecurity and ensuring that cyber threats

are identified and tracked as part of the overall security risk assessment and the plan would help enhance the facility's perimeter and boundary.

Another result of this study was the impact part-time, third-party security personnel has on the security plan. Most venues outsource their security services to a third party and conduct background checks on temporary and permanent employees. Directors of venues made measures to alleviate staffing shortages, mainly by boosting hourly wages. Training requirements for security personnel included familiarization with the location or event, forbidden objects, fan code of behavior, standard operating procedures, how to use security technology, and crowd control.

Facility and security management leave cybersecurity to different departments within the organization or outsource it. The current research uncovered that several participants from the facility management profession needed to understand cybersecurity and its impacts on their overall security plan. Multiple cybersecurity personnel interviewed as part of this research recommended that facility and security management play a more significant role in cybersecurity and understand the impact a cybersecurity breach could have on the facility.

Sports facility management and security personnel provide a safe and friendly environment for the fans, players, and staff, which is one of their priority tasks. However, they must continue growing their knowledge and experience, incorporate better communication up to the league level across the local community (other professional teams and venues), and share information to increase their security posture.

References

Birns, R., Southwell, A., & Arad, B. (2016). How a new defensive line can protect sports properties. *Street & Smith's Sports Business Journal, 19*(20), 14.

Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology. 3*(2), 77–101. https://doi.org/10.1191/1478088706qp063oa

Cleland, J. (2019). Sports fandom in the risk society: Analyzing perceptions and experiences of risk, security, and terrorism at elite sports events. *Sociology of Sport Journal, 36*(2), 144–151. https://doi.org/10.1123/ssj.2018-0039

Creswell, J. W., & Poth, C. N. (2018). *Qualitative inquiry and research design: Choosing among five approaches* (4th ed.). Sage.

Crotty, M. (1998). *The foundations of social research: Meaning and perspective in the research process*. Sage.

Crumley, B. (2022). Intrusive drones defy airspace bans at NFL, NCAA football games in Seattle. https://dronedj.com/2022/09/26/intrusive-drones/

Cybersecurity & Infrastructure Security Agency. (2022, June 24). *Stadium spotlight: Connected devices and integrated security considerations*. https://www.cisa.gov/stadium-spotlight-connected-devices-and-integrated-security-considerations

DarkTrace. (2021). *2021 threat report: Four key trends in the cyber-threat landscape*. DarkTrace.

Department of Homeland Security Center of Excellence. (2013, July 1). *Best practices in anti-terrorism security for sporting and entertainment venues resource guide*. https://www.safetyact.gov/externalRes/refdoc/CCICADA%20BPATS.pdf

Department of National Intelligence. (2016, January 1). *Year 2015. Counter terrorism guide historic timeline*. https://www.dni.gov/nctc/timeline.html

Duckworth, A., & Krieger, J. (2021). The world will be watching and so will NSA!': A history of technology and security at the Olympic Games. *The International Journal of the History of Sport, 38,* 264–281. https://doi.org/10.1080/09523367.2021.1909574

Dyer, J. T., & Cussen, R. B. (2019). How to strengthen your facility's perimeter security. *Athletic Business,* 36–40.

ESPN. (2022, February 13). *San Francisco 49ers' network hit by gang's ransomware attack; team notifies law enforcement*. https://www.espn.com/nfl/story/_/id/33283115/san-francisco-49ers-network-hit-gang-ransomware-attack-teamnotifies-law-enforcement

Federal Bureau of Investigation. (2018, November 1). *InfraGard*. Washington, DC, United States.

Greenwald, M. (2017, December 1). *Cybersecurity in sports: Questions of privacy and ethics*. https://www.cs.tufts.edu/comp/116/archive/fall2017/mgreenwald.pdf

Grow, N., & Shackelford, S. J. (2020). The sport of cybersecurity: How professional sports leagues can better protect the competitive integrity of their games. *Boston College Law Review, 61*(2), 473–522.

Hall, S. (2010, June 1). *Sport event safety and security: The importance of training your people*. https://www.securitymagazine.com/articles/80915-sport-event-safety-and-security-the-importance-of-training-your-people-1

Hall, S. A., Fos, P. J., Marciani, L., & Zhang, L. (2011). Value modeling in sport security planning: Setting priorities in security efforts at large spectator sports. *International Journal of Sport Management, 12,* 191–207.

Jayawardhana, A. (2016). Ensuring security against the threats of terrorist acts in mega sport events. *International Journal of Sport Management, Recreation & Tourism, 25,* 1–8.

Jones, I. (2015). Research methods for sports studies. Routledge.

Kvale, S. (1996). *Interviews: An introduction to qualitative research interviewing.* SAGE Publications.

Martin, C., & Robertson, R. (2020). *The cyber threat to sports organisations*. United Kingdom: National Cybersecurity Centre.

Merriam, S. B., & Tisdell, E. J. (2016). *Qualitative research: A guide to design and implementation* (4th ed.). Jossey-Bass.

National Center for Spectator Sports Safety and Security (NCS4). (2021). *2021 spectator sports safety & security survey.* The University of Southern Mississippi. https://ncs4.usm.edu/research/industry-reports/

National Center for Spectator Sports Safety and Security (NCS4). (2022). *Venue security director survey.* The University of Southern Mississippi. https://ncs4.usm.edu/research/industry-reports/

Popper, D. (2015, November 15). NFL says 'no known threats against NFL stadiums' in wake of Paris terrorist attacks. *New York Daily News*. https://www.nydailynews.com/2015/11/15/nfl-says-no-known-threats-against-nfl-stadiums-in-wake-of-paris-terrorist-attacks

Proof Point. (2022, January 1). *Insider threat*. https://www.proofpoint.com/us/threatreference/insider-threat

Schmidt, M. (2015, June 16). Cardinals investigated for hacking into Astro's database. *The New York Times*. https://www.nytimes.com/2015/06/17/sports/baseball/st-louis-cardinals-hack-astros-fbi.html

Shein, M. (2021, June 4). The NFL's GSOC takes center stage in getting players back on the field. *Security Magazine*. https://www.securitymagazine.com/articles/95338-the-nfls-gsoc-takes-center-stage-in-getting-players-back-on-the-field

Sky Safe. (2023). *Flag on the play. Drones create havoc for sporting events*. https://www.skysafe.io/blog/flag-on-the-play-drones-create-havoc-for-sporting-events

Smith, N. P., Bowers, A., Naquin, M., & Gillan, W. (2017). An analysis of the influence of the Boston Marathon bombing on sports venue management in the Gulf Coast States. *Sport Safety and Security, 2*(1), 1–14.

Tavella, D. F. (2010). Duty of care to spectators at sporting events: Unified theory. *Florida A&M University Law Review, 5*(2), 181–196.

Tie, Y. C., Birks, M., & Francis, K. (2019, January 2). Grounded theory research: A design framework for novice researchers. *SAGE Open Medicine*, 7. https://doi.org/10.1177/2050312118822927

Transportation Security Administration. (2019, October 1). *Protecting public areas best practices and recommendations.* Springfield, Virginia, United States.

United States Secret Service. (2020, August 1). Mass attacks in public spaces. https://www.secretservice.gov/sites/default/files/reports/2020-09/MAPS2019.pdf

Veselinović, J., Perović, A., Đukić, S., Mrdak, G., & Nikolić, M. (2020). Security management in sport. *Facta Universitatis, Series: Physical Education and Sport, 18*(2), 457–464. https://doi.org/10.22190/FUPES200630043V

Xu, X. (2018). Terrorism in major sports events: Difficult in maintaining security and countermeasures. *International Sports Law Review, 12*(3/4), 363–376.