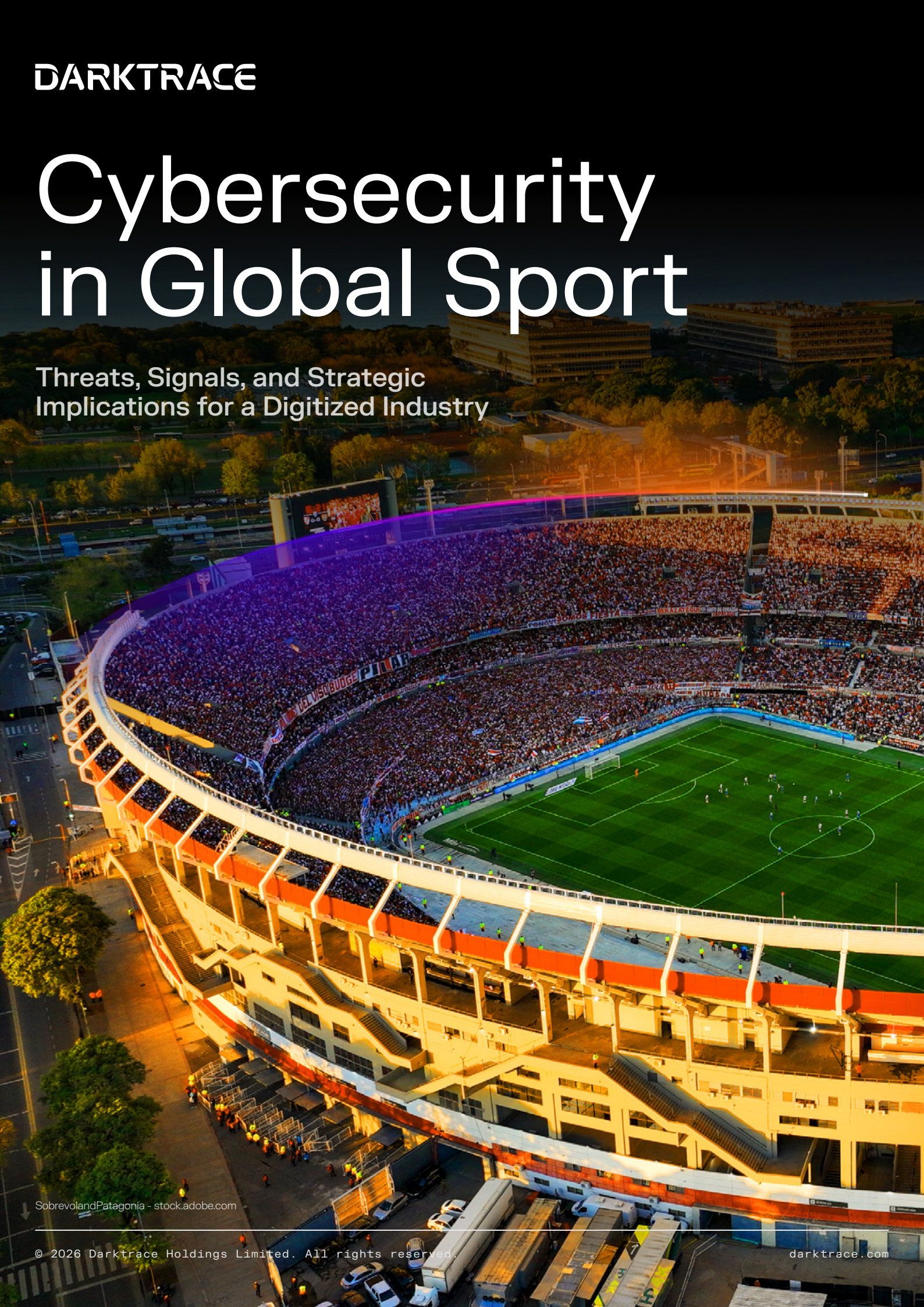
DARKTRACE

Cybersecurity in Global Sport

Threats, Signals, and Strategic Implications for a Digitized Industry



SobrevolandPatagonia - stock.adobe.com

Disclaimer

This report is for informational purposes only. Conclusions are made based on available data, which may change over time.

The views expressed in this report are those of the authors and do not necessarily reflect the views of any specific organization or governmental entity. The information in this report does not constitute legal, financial, or professional advice. The report does not guarantee the security of any systems, and ongoing vigilance and adaptive strategies are required to address emerging threats.

This report is provided "as is," without warranties or representations, express or implied, regarding accuracy or completeness. No liability is accepted for any damages or losses arising from the use or reliance on the content.

Overview

This report is intended to highlight the current challenges the global sporting sector faces and provide forward-looking views on future challenges as AI increasingly becomes adopted across the sector.

It examines incidents, telemetry, and case studies, and includes data from a survey of 875 IT cybersecurity professionals across sports organizations in the US, UK, Australia and Germany.

Authors

Ahmed Gardezi	Nathaniel Jones
Manoel Kadja	Emma Foulger
Justin Torres	Nicole Wong
Calum Hall	

Contents

Executive Summary

The global sports industry has undergone a rapid and continuous digital transformation.

Clubs, leagues, federations, and major sporting events now depend on complex ecosystems that span ticketing platforms, cloud services, broadcast networks, mobile applications, smart stadium infrastructure, and extensive third party supply chains. A new layer of exposure is now emerging as sports organizations adopt generative AI and agentic AI in areas such as fan experience, business operations, and beyond.

For a sector where trust, timing, and public visibility define impact, AI risk is becoming part of the broader cyber-resilience challenge.

While this transformation has enhanced fan engagement and operational efficiency, it has also expanded the attack surface far beyond traditional enterprise boundaries. The report examines incidents, telemetry, and case studies and includes data from a survey of 875 IT cybersecurity professionals across sports organizations in the US, UK, Australia and Germany.

The trends identified do not point to a singular adversary or campaign.

Instead, they reveal a consistent and escalating pattern: sport has become a persistent cyber target because of its global visibility, symbolic value, fixed operational timelines, and low tolerance for disruption.

Across the sector, Distributed Denial of Service (DDoS), ransomware, identity abuse, supply chain compromise, and large scale social engineering dominate observed activity, while geopolitical context primarily shapes adversary intent. Drawing on sector wide incidents, Darktrace data, practitioner insight, and lessons from major global events such as the Olympics, this report assesses how cyber risk in sport is evolving and why defensive strategy must shift from reactive incident response to structural resilience.

Key takeaways:

84%

84% of professional sports organizations surveyed have experienced at least one cyber incident in the past 12 months, with more than half (57%) hit multiple times. This underscores that cyber risk is already an operational issue for the sector.

34%

34% of respondents cited stadium operations as the most critical function to protect during a live event, reinforcing that cyber resilience in sport is defined by high-visibility moments where downtime is least acceptable.

19%

Darktrace sports sector customers received **19% more phishing emails** than non-sports sector customers, reinforcing that email and identity remain dominant attack vectors for sports organizations.

21%

37%

21% of phishing emails targeting sports sector customers were sent to VIPs, while 37% contained novel social engineering techniques, highlighting how attackers are focusing on high-value identities and adapting tactics to exploit urgency, trust, and operational complexity in the sports sector.

72%

72% of respondents believe AI will increase cyber risk over the next 12 months as AI adoption grows in high stakes areas including stadium operations, ticketing and fan engagement, and business operations.

47%

47% of respondents cited AI prompt risks and attacks and risks introduced during AI development & deployment as top concerns for AI use within their organizations.

Why the Sports Industry is a High Value Digital Target

Sport is no longer a discreet entertainment industry. It is a globally visible, data rich, and a politically resonant domain. Modern sporting organizations process sensitive personal data at scale, operate time critical systems in front of live audiences, and rely on sprawling vendor ecosystems to deliver broadcast, commerce, and fan engagement services.

International sporting events such as the Olympics or FIFA World Cup function as temporary, globally-distributed critical infrastructure, which spans governments, telecommunications providers, cloud platforms, stadium operators, broadcasters, and sponsors. As a result, cyber risk in sport resembles that of national infrastructure rather than that of a conventional commercial enterprise.

Sports organizations hold high-value information, including: fan data and athlete data, commercial negotiations, tactics, contracts, sponsorship information, and operational plans. The growing use of AI by threat actors alongside a larger attack surface because of rapid AI adoption by businesses raises the stakes around this data-rich environment. In this context, the risk is not only that AI systems are attacked directly, but that compromised identities and weak integrations increase risk of manipulation, data exposure, and more.

This context explains the breadth of observed cyber activity. Financially-motivated criminals pursue extortion and fraud; hacktivist groups seek visibility and disruption; and state aligned actors view major sporting events as opportunities for signaling, intelligence collection, or strategic interference. Sport is attractive not because it is vulnerable, but because it is uniquely visible and because failure is public.

According to the survey Darktrace commissioned of IT cybersecurity professionals across sports organizations in the US, UK, Australia and Germany, **84% of professional sports organizations** have experienced a cyber incident in the past 12 months.

More than half, 57%, were hit multiple times. Respondents cited that the average cyber incident cost sports organizations $169,000 over the past 12 months. However, the real financial impact compounds: 57% reported being hit more than once, and 43% reported between six and 10 incidents in a single year. For those organizations, the cumulative annual cost could climb to as much as $1.7 million each.

Threat Landscape Overview

In recent years, numerous sporting organizations and events have suffered cyber incidents that expose common structural weaknesses rather than novel techniques. Federations have experienced repeated breaches involving misconfigured APIs and credential reuse, resulting in the exposure of member and player data.

Clubs have suffered client-side payment skimming, ransomware outbreaks, and compromise of ecommerce infrastructure through third-party scripts. **Fan platforms and mobile applications** have been accessed via exposed keys and weak API security, placing large user populations at risk.

Rather than treating these as isolated cases, it is more useful to view them as a repeatable pattern:

Access → Leverage → Disruption

Use Cases

Geopolitically Motivated Sabotage and Coercion

In 2016, the **World Anti-Doping Agency (WADA)** confirmed that a Russia-linked cyber group, commonly referred to as "Fancy Bear" (APT28), compromised its Anti-Doping Administration and Management System (ADAMS), exposing confidential athlete medical data tied to the 2016 Summer Olympics in Rio De Janeiro. WADA assessed the intrusion as retaliatory following investigations into state sponsored-doping. The incident illustrates how cyber operations can be used to undermine institutional legitimacy and intimidate governance bodies through targeted data exposure. [1]

In February 2018, **the Olympic Destroyer malware** impacted civil services including Wi-Fi, ticketing, and broadcast systems during the Winter Games opening ceremony in PyeongChang, South Korea. It used administrative utilities and false-flag code to obfuscate attribution.

The operation is best characterized as deliberate sabotage, highlighting geopolitically motivated disruption. [2]

Governance Risk and Long Tail Exposure

Documents leaked via Der Spiegel's Football Leaks in 2018 formed the basis of an ongoing Premier League dispute against Manchester City Football Club, which remains unresolved at the time of writing [3]. The club maintains that the materials were unlawfully obtained and taken out of context. Irrespective of the outcome of the legal dispute, this incident underscores how cyber-enabled data exposure can escalate into long-tail legal and reputational risk [4].

Ransomware and Extortion

In November 2020, Manchester United Football Club confirmed a "sophisticated" cyberattack on its internal IT systems consistent with ransomware activity. Thanks to swift containment and proactive segmentation, match-day infrastructure remained unaffected. This incident underscores how targeted preparedness and tactical isolation can limit operational fallout, even in high-profile breaches. [5]

In April 2021, Babuk ransomware targeted the Houston Rockets of the National Basketball Association (NBA).

While internal defenses prevented full encryption, attackers claimed to exfiltrate approximately 500 GB of sensitive contracts, financials, and non-disclosure agreements (NDAs). The incident illustrates how data theft, independent of operational impact, can be weaponized to inflict reputational and financial harm. [6]

Data Loss (Identity and API Exposure)

In February 2025, the **French Football Federation (FFF)** disclosed a data breach resulting from a compromised account and a misconfigured Swagger UI API, enabling attackers to extract personal data relating to members, employees, and volunteers.

Later in November, stolen credentials were reused to access centralized club membership systems, exposing licensed player data nationwide. The recurrence of access driven compromise in these incidents indicates persistent targeting rather than isolated failure, **particularly sensitive ahead of France's involvement in the FIFA World Cup 2026.** [7]

Shadow AI and Emerging AI Risks

The sports industry is facing a new wave of cyber risk as organizations adopt artificial intelligence faster than governance can keep pace, while attackers use the same technology to launch faster, more convincing, and more disruptive campaigns.

At the center of the concern is **shadow AI**, the unsanctioned use of AI tools by employees or contractors without formal approval or oversight. In sport, that can mean sensitive information such as athlete health records, scouting notes, contract details, sponsorship negotiations, or internal strategy documents being entered into third-party AI systems. The result is a growing risk of data leakage, privacy breaches, and compliance failures at a time when teams, leagues, federations, and event operators are under pressure to move quickly and innovate.

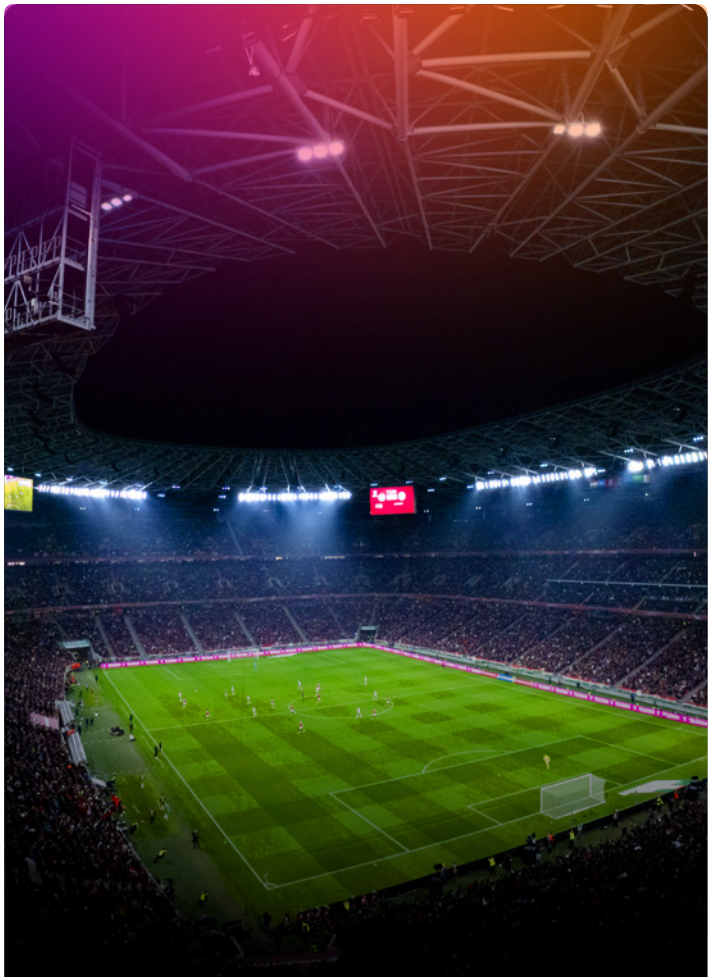
72%

72% of IT cybersecurity professionals from sports organizations surveyed believe AI will increase cyber risk over the next 12 months as AI adoption grows in high stakes areas including stadium operations, ticketing and fan engagement, and business operations.

34%

Stadium operations was identified by **34% of respondents** as the area that would have the greatest impact if compromised in a cyberattack, yet more than a third (35%) said they are currently using or plan to use AI in that area. This underscores the potential for increased cyber risk as the attack surface grows.

What makes the sports sector particularly vulnerable is the combination of live operations, high-profile brands, global audiences, and large volumes of personal and financial data. As AI adoption expands across performance analysis, customer engagement, and business operations, security controls, staff awareness, and data governance must evolve just as quickly.



In Summary

Individually, most of these incidents are unremarkable from a technical standpoint.

Collectively, they demonstrate persistence rather than opportunism. The same ecosystems are revisited over time, often in proximity to tournaments or periods of heightened public attention. This suggests a targeting calculus shaped by timing and impact, not just ease of access. Geopolitical context further colors this landscape.

International bans, sanctions, and regional conflict create incentives for cyber activity that extend beyond financial gain. While attribution is frequently inconclusive, the broader environment matters: sport offers adversaries a platform where disruption carries symbolic and psychological weight disproportionate to technical effort.

Supply Chain and Third Party Risk

Few sports organizations operate in isolation.

Ticketing providers, merchandise platforms, payment processors, analytics services, broadcast partners, stadium technology vendors, and managed service providers all form part of the operational fabric. Third parties often maintain persistent access, security maturity varies widely across vendors, and compromise of a single provider can cascade across multiple organizations simultaneously.

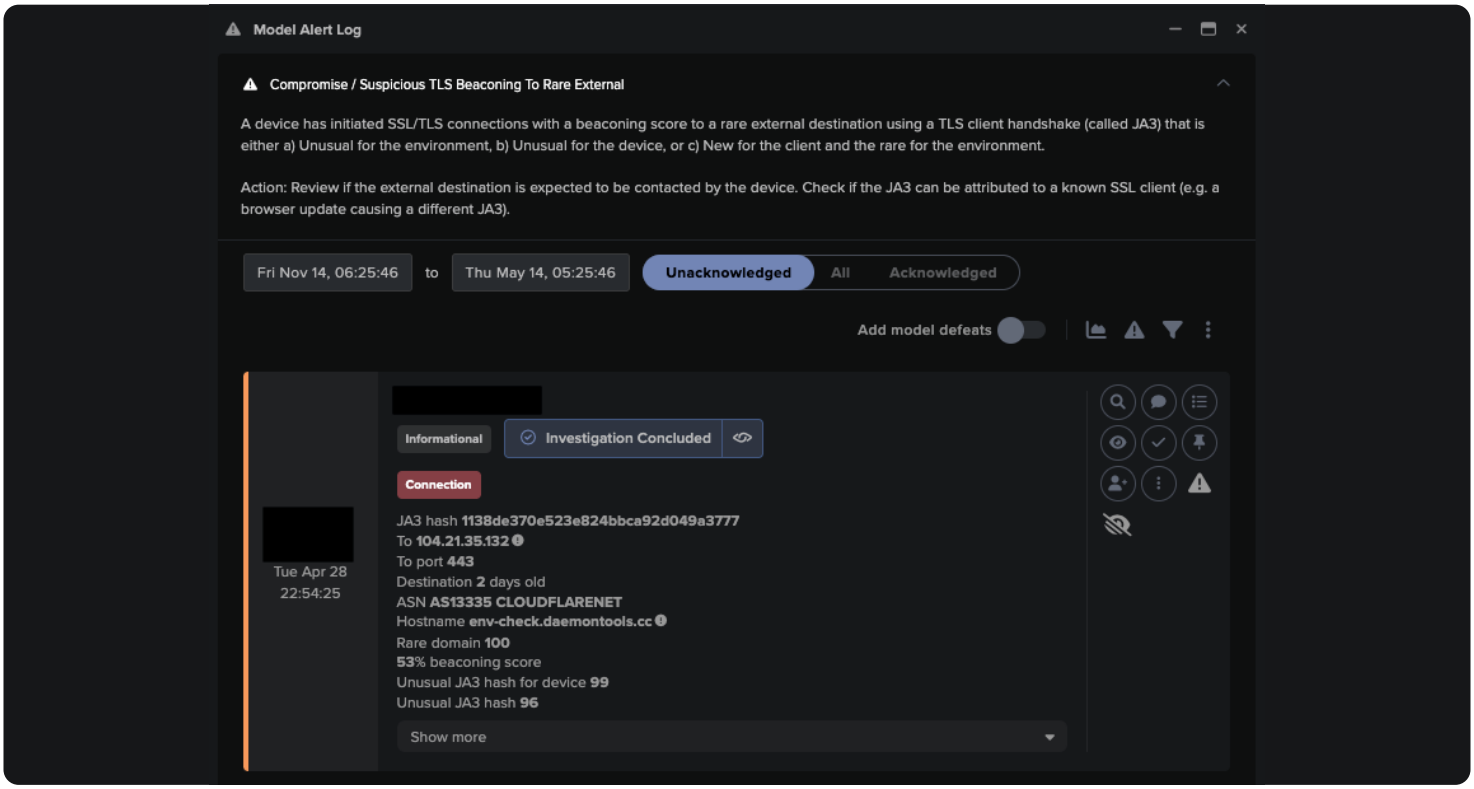
Historical incidents across multiple sectors show that long-term pre-positioning via trusted suppliers is one of the most effective ways to target high-profile operations. In many cases, the weakest point in an organization's security posture lies outside its direct control. **Sport is no exception, particularly given the required interconnectivity to host such large events.**

In 2018 ahead of the Winter Olympics in PyeongChang, reports surfaced that an IT partner to the International Olympic Committee was compromised months before Olympic Destroyer malware attack during the opening ceremonies [8].

The supplier hosted critical Olympic cloud infrastructure, and malware samples reportedly contained employee credentials, and reports suggested attackers may have used supplier access for reconnaissance or preparation. The incident showed how a trusted technology partner connected to a high-profile event could become a pathway into time-critical sporting infrastructure.

In April 2026, security researchers from Kaspersky identified a supply chain attack using **DAEMON Tools**, which is widely used software for managing disk-image files. [9] The researchers reported that attackers injected malicious code into signed DAEMON Tool installers, enabling information collection, and in some cases, delivery of a backdoor capable of downloading payloads and executing commands. Darktrace observed potential exploitation in a sports sector organization, including outbound beaconing to a rare endpoint that appeared to be associated with a malicious command and control (C2) domain associated with the exploit.

This reinforces the high level of risk associated with third-party software and the importance of ongoing behavioral monitoring to identify the earliest signs of a potential compromise.



Stadiums as Cyber-Physical Environments

Modern stadiums operate like small smart cities, with multiple network layers supporting everything from fan services to critical operations. At the front end, business IT systems handle ticketing, payments, mobile apps, and corporate functions, while public Wi-Fi networks provide connectivity to tens of thousands of fans.

Alongside these are systems for security and surveillance often incorporating Internet of Things (IoT) devices such as IP cameras, as well as operational technology (OT) controlling lighting, heating, ventilation and air conditioning (HVAC), and other building functions. Although these layers are meant to be segmented, in practice they are often interconnected through shared credentials, remote vendor access, or weak network separation, creating pathways for threat actors to move laterally between systems.

CCTV

Closed-Circuit Television (CCTV) systems in stadiums are typically built on networked IP cameras and video management platforms. These systems are used for real-time monitoring, but they also introduce a cybersecurity risk.

Many deployments, including those using widely available hardware from vendors, can be vulnerable to issues such as default credentials, exposed remote access services, and delayed patching. Threat actors have exploited these weaknesses by taking control of cameras to form botnets, by using compromised devices as entry points into the wider network.

Once breached, threat actors can move laterally to access other systems, disrupt monitoring, or create blind spots in physical security coverage. In a stadium context, this could disrupt security operations or provide entry to further attacks against ticketing, access control, or operational systems, potentially requiring the cancellation of the event for safety reasons.

In late 2024, the FBI warned about a HiatusRAT campaign targeting unpatched CCTV systems including Chinese-branded cameras. HiatusRAT is a Remote Access Trojan (RAT) that gathers system, network, processes, and file system information and exfiltrates the data. In early 2025, the US Department of Homeland Security issued a threat advisory regarding interconnected cameras made from China that provided the ability "to conduct espionage or disrupt US critical infrastructure." [10] The lesson is not about vendor nationality, but instead that poorly secured surveillance devices represent a durable, low cost ingress point for a wide range of actors.

That can range from financially motivated groups to state aligned operators seeking quiet, persistent access—particularly in high visibility environments such as major international sporting events.

Building Management Systems

Building Management Systems (BMS), including HVAC and lighting, present a similar risk within stadium environments. These systems are often connected to central networks for monitoring and remote maintenance, and sometimes via third-party vendors.

In 2013, a breach of U.S. retailer Target occurred where threat actors gained initial access through credentials stolen from an HVAC contractor before moving laterally into payment systems [11]. While not specifically targeting HVAC systems, the same architecture is commonly used in large venues where contractors may retain persistent remote access. This can create an entry point for threat actors, especially if access controls, or authentication mechanisms are weak.

Interconnected Stadium Ecosystems

The primary risk within stadium IoT and OT environments is not necessarily a vulnerable device, but the interconnection of systems. Public Wi-Fi, CCTV networks, BMS, and corporate IT are often using shared physical networks and infrastructure, enabling attackers to move across the environment and VLANs once accessed.

The 2022 FIFA World Cup in Qatar demonstrated how modern venues are becoming centrally managed cyber-physical systems rather than standalone stadiums. The tournament introduced the world's first "connected stadium" concept, with all eight stadiums managed through a single unified technology platform from Doha's Aspire Command Centre [12]. That environment covered everything from lighting and access gates to communications and IT, with each stadium supported by a digital twin to help security teams detect and mitigate issues as they emerged. The model created major operational benefits but also could concentrate risk by increasing the attack surface (over IP).

For defenders, the key point is not "secure every device." It is "constrain interconnection." Visibility across IT and OT, disciplined third-party access, and strong identity controls matter more than perfect patching—because lateral movement is what turns a small foothold into event-impacting disruption.

Darktrace Telemetry: What the Data Shows

Darktrace observations across the sports sector provide empirical insight into how adversaries exploit these environments.

Email and Identity Abuse

Email remains the dominant initial access vector. Observed patterns include logins from rare geographies and autonomous systems, creation of inbox rules to hide responses or security notifications, and deletion of sent messages to evade detection. In several cases, attackers used compromised accounts to distribute further phishing or conduct internal reconnaissance.

A notable proportion of malicious email successfully passes authentication controls such as DMARC. Rather than relying on spoofed domains, adversaries increasingly leverage legitimate infrastructure and trusted platforms, exploiting human trust rather than technical weakness.

Darktrace Identity Abuse Patterns

- **Multiple logins** from rare IP addresses and ASNs
- **Inbox rules** created to hide replies and security alerts
- **Deletion** of sent phishing emails to avoid detection
- **Rapid pivot** from access to internal reconnaissance

Phishing at Scale

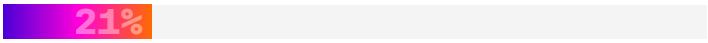
Across a six month period from October 2025 through March 2026, Darktrace detected more than 116,000 phishing emails targeting customers in the sports sector, with executives and VIPs disproportionately targeted.

Phishing campaigns involving the use of QR codes and novel social engineering techniques increased significantly in Q1 2026 compared to Q4 2025, while overall phishing volumes exhibited seasonal spikes aligned with holidays and major events. Although overall volumes fluctuated at certain points, the effectiveness of phishing increased, with higher portions passing authentication and evading traditional security controls.

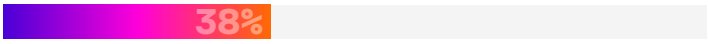
When exploring the disparity of email threats between sports and non-sports sectors, at the typical mailbox level Darktrace sports sector customers received **19% more phishing emails** than non-sports sector customers.

To this point, sports-focused vendors likely experience an increase in targeting due to their **mailboxes being tied to high traffic events** (i.e., games, ticket sales, merchandise drops, sponsorships), predictable seasonal spikes, and large external user interaction. Attackers look to exploit using social engineering, and credential harvesting campaigns that blend into legitimate high velocity email flows.

Over the six months of October 2025 and March 2026, Darktrace / EMAIL detected over 116,000 phishing emails across global sports-sector customers. Analysis of these emails reveals the following statistics:



21% of **phishing emails sent to VIPs**
(over 23,000 VIP phishing emails detected)



38% of malicious emails detected
were spear-phishing attempts

3% (over 3,900) of phishing emails
included newly created domains

3.5% (over 4,100) of phishing
emails included QR codes

84% of malicious emails detected by Darktrace
successfully passed DMARC authentication

37% of detected emails contained
novel social engineering features

The volume of phishing emails was more than 10% higher between October and December 2025 than between January and March 2026. This increase aligns closely with the seasonal holiday uptick seen across Darktrace customers globally, as previously discussed in Darktrace's Annual Threat Report 2026, and reflects broader email trends associated with Black Friday and the holiday season.

While overall phishing volumes declined in the first quarter of 2026, there were notable shifts in the types of phishing observed compared with the final quarter of 2025.

- **87% of phishing emails** passed DMARC authentication in this period
- The number of QR code phishing emails **rose by 33%**
- The number of phishing emails containing novel social engineering features **rose by 4%**

Threat actors are no longer relying on spoofed domains and instead look to leverage legitimate third-party platforms and authenticated domains to increase user trust. Despite a reduction in overall phishing emails at the start of 2026, there was a rise in those utilizing QR codes and novel social engineering techniques.

This may reflect the wider uptake of newer technologies within sports environments; as technology like QR codes become the norm for ticketing, sharing links, and passing on information within these environments, user awareness of associated risks decreases.

Email threats continue to exploit the urgency, brand trust, operational complexity, and fast-paced nature of the sports sector, rather than relying on technical weaknesses alone.

Ransomware and Pre-Positioning

Ransomware incidents in the sports sector consistently show signs of deliberate planning rather than opportunism. Observed activity includes the first-time use of highly privileged credentials on affected devices, lateral movement via standard administrative protocols, and data exfiltration prior to encryption.

These patterns indicate dual objectives: theft of sensitive data and operational leverage. In one case observed by Darktrace, evidence suggests that attackers maintained access for weeks before executing ransomware, reinforcing the importance of early detection.

Case study

In April 2025, within the deployment of a sports sector customer, a device believed to be a database server was observed making unusual use of a highly privileged administrative credential.

Shortly thereafter, the device initiated an unusual volume of SMB activity, including the renaming of files with newly added extensions. Notably, the **'LYNX' file extension**, commonly associated with Lynx ransomware, was observed, indicating file encryption. Files named 'README.txt' were also observed, likely representing ransom notes.

Around the same time, a second server device was seen using the same highly privileged credential, performing actions consistent with network reconnaissance and lateral movement over DCE-RPC. Further file encryption and reuse of the compromised credential were subsequently observed on additional devices as the threat actor moved through the network. Likely data exfiltration was identified from one of the devices involved, with an anomalous upload of more than 2 GB to various rare external endpoints, including some associated with the cloud storage service MEGA.

Two weeks prior to these events, the initially involved database server was seen sending data externally to a **rare external IP geolocated in Russia**. This IP was heavily flagged by open-source intelligence (OSINT) for its associations with various kinds of malicious behavior throughout 2025. This activity may have represented preparatory staging and planning by the threat actor before the attack was executed at full scale.

Darktrace Ransomware Indicators

	Use of **privileged administrative credentials**
	Lateral movement across internal servers
	Data exfiltration prior to encryption
	File renaming associated with known ransomware families

Mega-Events and the World Cup Effect

Historical data from the Olympic Games and previous global tournaments consistently show that cyber activity scales with visibility.

The upcoming 2026 FIFA World Cup, hosted across Canada, Mexico and the US, represents an unprecedented attack surface: a month long event spanning three nations and dozens of host cities, with a digital footprint and complex supply chain that extends far beyond stadium boundaries into transportation networks, hospitality, broadcasters, sponsors, municipal infrastructure, and more.

World Cup-specific risk vectors include deep dependence on **cloud and Software-as-a-Service (SaaS) platforms,** extensive smart stadium and OT deployments, broadcast and streaming ecosystems with global reach, and large-scale fan-centric fraud tied to tickets, travel, accommodation, and unofficial merchandise. These risks are further compounded by a fragmented operational environment, in which security ownership is distributed across national, state, city, private operators, and commercial partners.

Geopolitical signaling further elevates the threat profile. Previous international sporting events have demonstrated that nation-state actors use the cyber domain to signal intent, influence narratives, or retaliate symbolically.

In the context of the 2026 World Cup, Russia's continued exclusion from international sport, the ongoing conflict in Ukraine, US defensive support to Ukraine, and Iran's likely participation in the tournament introduce additional motivations for state-aligned and non-traditional affiliated actors to operate below the threshold of armed conflict.

The result is a materially higher likelihood of disruptive, deniable, and psychologically resonant cyber activity targeting visibility, trust, and continuity rather than purely technical impact.

Key Lessons from Supporting Major Global Sporting Events

Darktrace has supported multiple global sporting events where cyber risk is amplified by timing, visibility, and geopolitical attention, including supporting sports-sector customers during the Paris 2024 Summer Olympic Games and the 2024 UEFA European Championship, as well as the 2022 Qatar World Cup. In addition to the use of Darktrace's products, Darktrace's cyber analysts were embedded across threat research, 24/7 SOC operations, and consultancy to provide multi-domain support before and during these events.

During the preparatory phase, Darktrace's cyber analysts supported the identification of high-value assets and alignment of detection priorities and workflows to relevant attacker tradecraft.

This was driven through operational and strategic intelligence and was paired with continuous monitoring of open-source reporting for developments with direct defensive relevance, allowing teams to anticipate how public narratives, political signaling, and operational milestones could translate into attacker behavior before it manifested on customer networks. Analysts also performed behavioral-based threat hunts, such as DNS entropy analysis to surface abnormal spikes in DNS activity, to uncover misconfigurations enabling traffic to bypass expected security controls.

During live events, this shifted into sustained threat hunting, risk-based triage of behavioral detections, and close coordination with customer event stakeholders, private and government partners and incident management teams. Critical event milestones that would allow even modest actions from attackers to have outsized impact, such as event opening and closing ceremonies and finals, were influential to define periods of heightened awareness.

Darktrace's analyst support also extended to key supply chain stakeholders. Analysts closely monitored customers affiliated with the events, prioritized high-confidence behavioral detections as they emerged, and tracked abuse of event-themed infrastructure, including event-related typosquatting and anomalous external connectivity.

Across both events, a pattern was clear: operationally, the threat landscape extends far beyond a single stadium or network.

Digitized venues, IT/OT convergence, and temporary connectivity from vendors, contractors, and spectators expands the attack surface from event organizer headquarters to stadium turnstiles, display systems, and broadcast infrastructure. This renders static asset inventories and rule-based controls insufficient in these dynamic environments.

Crucially, security teams must account for the human element: during high-pressure live events, even experienced engineers and operators are working under time constraints and fast-paced environments, increasing the likelihood of workarounds and human error. Real-time anomaly detection was essential to detect these cases before they escalated into operational impact during live events. Successful defense depended on close collaboration beyond the security team, ensuring engineers, infrastructure teams, and third party vendors could act quickly and decisively when minutes mattered most.

Across high-profile events, Darktrace's experience shows that effective cyber defense includes preparation, real time visibility, and the ability to respond dynamically and decisively when timing, complexity, and public exposure converge.

Pre-Event Threat Intelligence: Honeypots

In advance of the FIFA World Cup 2026, Darktrace has deployed dedicated honeypot environments designed to replicate the IT and OT architecture of modern stadiums, including CCTV networks, BMS/HVAC systems, and public-facing infrastructure.

These environments are not defensive controls; they are observation points to understand how attackers approach stadium environments: where they probe first, how they attempt initial access, and how quickly they pivot between IT and OT layers. Early observations show consistent patterns of opportunistic scanning against exposed services, followed by credential-based access attempts and low-noise reconnaissance designed to persist ahead of major events.

Any valuable intelligence observed will feed directly into the sporting and broader CNI community, particularly around early-stage behaviors such as rare external connectivity, abnormal service access, and credential misuse across segmented environments. In the context of live events, where response time is constrained, these early indicators are often the difference between contained activity and operational disruption.

A CISO's View: Protecting the Modern Sporting Stadium

An interview with Karim Benslimane, VP and Field CISO at Darktrace; Former CISO and Lieutenant-Colonel (RC) at COMCYBER-MI. Karim has led major IT and cyber security projects for international arenas and events such as the **Football World Cups, Rugby World Cups, World Athletics Championships and over 500 events.**

Protecting major stadiums and venues during global sports events like several football and rugby World Cups reinforced a simple truth: these environments are critical national assets— they are time critical, highly-visible and crucial systems of systems. A stadium is simultaneously a city, a broadcast hub, a transport node, a public safety space, and a national symbol. That makes them attractive not just to criminals, but to **politically-motivated and state-aligned actors** willing to plan years ahead.

The greatest risk does not come from loud, last minute attacks. It comes from quiet pre-positioning: compromises in supply chains, trusted vendors, or operational technology that only activate once the stadium is live. Modern venues depend on tightly interconnected IT and OT: access control, lighting, CCTV, screens, HVAC, ticketing, and Wi-Fi. If segmentation is weak, a single foothold can cascade across the environment.

Live events impose brutal constraints. You do not have hours to analyze alerts during a match — you have minutes. That reality breaks manual, rules-based security models. Defense must be everywhere (outside and inside the venue) behavioral, continuously aware of what "normal" looks like in a stadium, and capable of decisive action without human delay.

Ultimately, success depends on preparation: resilient architecture, visibility across IT and OT, disciplined third-party access, and teams that understand stadium operations as deeply as cybersecurity. In these environments, prevention and readiness matter far more than hindsight.

"The most dangerous attacks on major sporting events are silent, supply-chain driven, and triggered exactly when **failure is least acceptable**."

Strategic Implications for the Sports Industry

Several themes emerge consistently across incidents, data, and practitioner insight:

	Architecture matters more than attribution
	Supply-chain discipline is foundational
	Identity is the primary control plane
	IT and OT cannot be secured independently
	Time pressure defines impact

Organizations that treat cyber risk as an IT issue will continue to be surprised. Those that treat it as an operational and governance challenge are better positioned to withstand disruption. As digitization accelerates, risk will continue to rise unless defensive maturity keeps pace.

Priority actions include:

01 Threat modeling for emerging technologies, including AI misuse

02 Rigorous supply chain governance and vendor access control

03 Strong segmentation across IT, OT, and fan-facing systems

04 Identity-centric security with anomaly detection and universal multi-factor authentication (MFA)

05 Phishing resilience across all channels, including QR-based vectors

06 Operational playbooks aligned to live event constraints

The global sports industry is entering a new phase of exposure. The question is not whether cyber incidents will occur, but whether organizations are structurally prepared to absorb them without cascading operational, reputational, or governance failure. The path forward lies in addressing the conditions that make sport such a compelling target in the first place. Preparation, not prediction, will define resilience.

In a sector where disruption is highly visible and recovery windows are narrow;
cybersecurity must be embedded long before the opening whistle.

References

01 https://www.wada-ama.org/en/news/wada-confirms-another-batch-athlete-data-leaked-by-russian-cyber-hackers-fancy-bear

02 https://cyberlaw.ccdcoe.org/wiki/Olympic_Destroyer_%282018%29

03 https://www.espn.com/soccer/story/_/id/48024829/premier-league-manchester-city-charges-analysis-hearings-gab-marcotti

04 https://www.spiegel.de/international/topic/football_leaks/

05 https://www.manutd.com/en/news/detail/official-manchester-united-club-statement-20-november-2020

06 https://www.infosecurity-magazine.com/news/cyberattack-on-nba-team/

07 https://www.bleepingcomputer.com/news/security/french-football-federation-fff-discloses-data-breach-after-cyberattack/

08 https://cyberscoop.com/atos-olympics-hack-olympic-destroyer-malware-peyongchang/

09 https://www.kaspersky.com/blog/daemon-tools-supply-chain-attack/55691/

10 https://abcnews.com/US/internet-connected-cameras-made-china-spy-us-infrastructure/story?id=118533418

11 https://krebsonsecurity.com/2014/02/target-hackers-broke-in-via-hvac-company/

12 https://www.darktrace.com/blog/how-darktrace-ai-helped-protect-the-qatar-world-cup-2022-from-cyber-disruption

Methodology

Darktrace's Threat Research Methodology

Darktrace's Threat Research team performs comprehensive analysis across aggregated customer telemetry to identify active threat activity, extract high fidelity indicators of compromise (IoCs), and generate actionable threat intelligence.

This research leverages Darktrace's anomaly-based detection and involves thorough analysis and contextualization by the Threat Research team. Detected threats are promptly reported to the relevant customer security teams. When a customer has Darktrace's Autonomous Response technology enabled, these threats are swiftly mitigated to prevent escalation. As noted in the Executive Summary, the incidents, telemetry, and case studies analyzed in this report do not attribute to a single threat actor or coordinated campaign.

All insights from Darktrace's analysis are based on detections and specific data from our AI-driven applications and anomaly investigations.

Sector Analysis Methodology

Throughout this report, sectors and industries are categorized using the Standard Industrial Classification (SIC) framework to ensure a consistent and standardized methodology for organizational classification.

For clarity and consistency, sector and industry labels are capitalized when referenced as formally defined SIC categories. Darktrace customer deployments within the sports sector were identified through belonging to specific relevant SIC categories, including SIC Classes 9312, 9319, 9311, 3012, 3949, and 4763. When interpreting sector level insights and statistical findings presented, readers should note that while the analysis is broadly representative of global threat trends, it is influenced by the underlying distribution of Darktrace customer telemetry across sectors.

Darktrace Telemetry: Email Trends and Analysis Methodology

The email-based statistics within this report are derived from analysis of monitored Darktrace / EMAIL™ model data for all sports sector customer deployments hosted in the cloud between October 1, 2025, and March 31, 2026 (Q4 2025 & Q1 2026). Around 90% of the global Darktrace customer base's email environments are cloud-based.

For the purpose of this report, and indeed Darktrace's analysis of email environments, "phishing indicators" refers to emails that are confirmed as malicious, as opposed to merely unwanted spam emails, while "phishing emails" refers to emails containing "phishing indicators."

Comparisons of phishing email activity between sports and non-sports sector clients were carried out through calculation of median phishing email rates since July 2025 per 100 mailboxes, taking into account variation in deployment sizes, and providing values for the typical phishing email rates at a mailbox level. At the typical mailbox level, sports sector mailboxes receive materially more phishing emails (approx 19%), indicating the difference is not driven by a few small or anomalous clients.

Survey Methodology

Findings based on survey of 875 IT cybersecurity professionals based in the US, UK, Australia and Germany, working in professional sports organizations (including clubs, societies & sporting bodies) employing 10+ people. The survey was fielded between May 28, 2026 and June 3, 2026 by independent market research agency, Opinion Matters. Average cyber incident costs were reported in local currency (USD, GBP, AUD, EUR) and converted to USD at exchange rates as of June 3, 2026.

About Darktrace

Darktrace is a global leader in AI for cybersecurity that keeps organizations ahead of the changing threat landscape every day. Founded in 2013 in Cambridge, UK, Darktrace provides the essential cybersecurity platform to protect organizations from unknown threats using AI that learns from each business in real-time. Darktrace's platform and services are supported by 2,300 employees who protect nearly 10,000 customers globally. To learn more, visit darktrace.com.

North America: +1 (415) 229 9100 | Europe: +44 (0) 1223 394 100 | Asia-Pacific: +65 6804 5010 | Latin America: +55 11 4949 7696

darktrace.com | info@darktrace.com