The Hidden Opponent:

Cyber Threats in Sport

nccgroup

People powered, tech-enabled cyber security

PHOENIX
SPORT & MEDIA GROUP

Overview

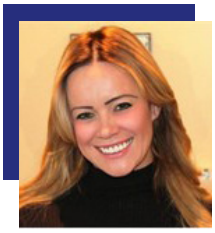
The aim of this report is to help organisations and individuals involved in the world of sport to understand their levels of cyber security vulnerability and exposure against the ever-evolving technology and threat landscape. Moreover, this report aims to signpost sports organisations and sportspeople to pragmatic advice and guidance on how to minimise their cyber security risks, helping to preserve brand reputation, confidentiality, integrity and availability of data, IT and other connected systems and assets.

This report is underpinned by qualitative and quantitative research performed by a team of researchers from the University of Oxford's Researcher Strategy Consultancy, in collaboration with global cyber security and risk mitigation experts NCC Group, and Phoenix Sport & Media Group. Interviews were held with key personnel involved in managing IT and cyber security in the world of sport; non-exhaustively this included insight from personnel working in professional football, rugby, Formula 1 racing, horseracing, cricket and tennis.

Contents

Foreword

Matt Lewis
Global Head of Research
NCC Group



Carly Barnes
CEO
Phoenix Sport & Media Group

In 2026 the global sports industry is projected to generate more than $700 billion (USD) in revenue. The vast amount of money involved in the world of sport presents an attractive and potentially lucrative opportunity for cyber criminals through fraud and extortion; the consequences of which could be damaging both financially and reputationally for sports organisations and individuals.

The cyber security risks facing the world of sport are compounded through continuous digital transformation. This includes everything from vast amounts of connected health technology used to monitor and appraise the fitness and performance of sportspeople, through to connected smart stadiums with technology such as smart turnstiles and barriers, CCTV and facial recognition, automated pitch temperature control and connected floodlights to name but a few.

The world of sport is therefore highly connected, the complexity of which hugely increases the attack surface and opportunity for financial-based attacks such a ransomware or business fraud, data protection violations through data breaches (deliberate or accidental) and in the realm of connected stadiums and automated barriers, the potential for impact on physical safety where those mechanisms might fail accidentally or through deliberate cyber attack.

Understanding cyber threats and implementing an effective risk mitigation strategy is a challenge that many sports organisations do not either have the expertise, resources or time on which to focus. It's important that we gain an understanding of what the current state of play is across all facets of sport so that we can understand current levels of maturity, and thus what organisations and individuals need to do to improve their cyber security posture and risk management strategies.

In this report, we are looking to drive awareness of cyber security and the importance of being more proactive and less reactive to cyber-attacks in professional sport. We want to help sports teams, venues and individuals build a sustainable industry that can cope with the ever-increasing and evolving digital world in which we live. By building awareness and helping to drive action, we can ensure sports organisations, venues and events remain available, accessible, safe and secure in the face of pervasive cyber threats.

Cyber Security in Sport

The world of sport is constantly changing with technological advancements. Vast amounts of data (much of which is personal and sensitive) is generated and processed in the world of sport, while vast amounts of money are moved around in various sports-based transactions. Most things are now connected in the world of sport. From fitness trackers to drones used for real-time telemetry on sportsperson performance, CCTV, facial recognition and smart turnstiles at sporting arenas, e-tickets and e-commerce for fans to purchase season tickets and merchandise, to name but a few. The connected nature of sport demands good cyber security practices since there are many different threat actors with different motives within the sporting domain, and the consequences of failing to secure systems and data can be significant through regulatory fines and reputational damage. Just ten real world cyber security incident examples from recent years, as found in our open-source literature review, include:

- Microsoft reported in 2019 on how Russian state hackers attacked the computers of at least 16 national and international sports and anti-doping organisations. Around the same time, the World Anti-Doping Agency (WADA) discovered that failed drug tests of Russian athletes had been erased from a critical data set.

- In 2019, a drone with live video feed was used in an attempt at gaining a betting advantage for an in-running horse race bet. In-running or in-play bets allow for betting while a sports game or race is in play and with dynamically changing odds. Live drone footage can be seconds quicker than live TV feeds of the same sporting event, thus providing gamblers with a significant edge. This example demonstrated the shifting landscape of gambling and how technology is providing mechanisms for gaining significant advantage.

- In 2019 the Instagram account of Wimbledon champion Simona Halep was hacked and used in an attempt to deceive her 1.3m followers into donating money to fraudsters.

- In a 2020 NCSC research survey, at least 70% of sports organisations experienced a cyber incident or breach, with approximately 30% of those incidents causing an average financial damage of £10,000 per incident. The biggest single loss for one sports organisation was over £4m.

- In 2020, NCSC also reported that the email address of a Premier League club's managing director had been hacked during a transfer negotiation and only intervention from the bank prevented the club from losing around £1m. Additionally, the same report mentioned an English Football League (EFL) club that had fallen victim to a ransomware attack, leaving the club unable to use their corporate email. The club's stadium CCTV and turnstiles were also affected by the ransomware, since they were connected to the same network, rendering them non-operational and almost resulting in a fixture cancellation.

- Since 2021, "Project Red Card", led by former Cardiff City manager Russell Slade has been threatening legal action against major gaming, betting and sports data companies over alleged unlawful selling of personal information and performance statistics of players. The project continues to gain support from hundreds of players across football and cricket demanding compensation for the trading of their data in a £500m lawsuit.

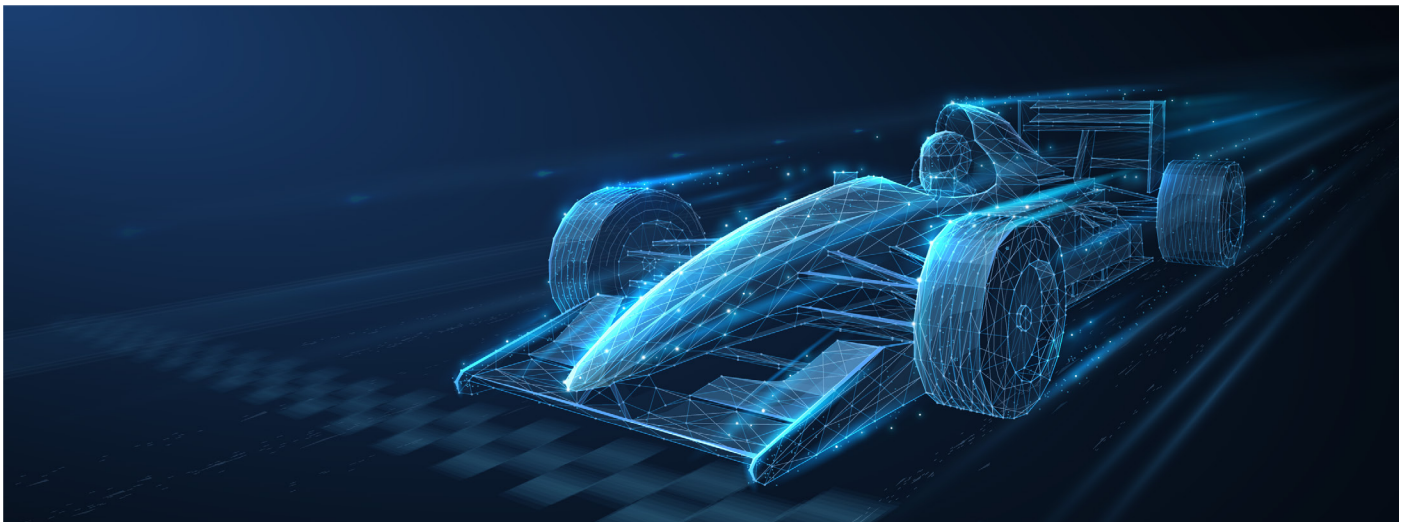
- In 2021, Liverpool FC captain Jordan Henderson handed over control of his social media accounts to anti-cyber bullying charity The Cybersmile Foundation to help tackle online abuse and provide support to victims of cyber bullying and online hate campaigns. Henderson has been a long campaigner in the fight against rising levels of abuse and discrimination within the game of football.

- In 2022, The Royal Dutch Tennis Association ("KNLTB") was fined a total of €525,000 by the Dutch Data Protection Authority, for selling the personal data of more than 350,000 of its members to sponsors.

- In 2022, The Sunday Times and Bureau of Investigative Journalism exposed an India-based computer hacking gang for hire, employed by a range of individuals and organisations to disrupt or influence the world of sport. Examples include critics of Qatar being hacked in the run up to the 2022 World Cup, former head of European football Michel Platini being hacked shortly before he was due to talk to French police about corruption allegations concerning the 2022 World Cup, and Formula 1 motor racing bosses Ruth Buscombe (head of race strategy for Alfa Romeo) and Otmar Szafnauer (CEO of the Aston Martin team) each falling victim to the hacking of their email accounts.

- In 2022, football fans were urged to be wary of ticket scams as fraudsters were using social media to offer fake tickets and deceive unsuspecting victims out of their money, with an average loss of £410 per fan. The surge in this type of fraud was attributed to fraudsters taking advantage of people desperate to attend live events following the end of COVID restrictions.

From just these ten examples, we see common themes around fraud and serious financial and operational impact to sports organisations following cyber attacks. We see that data protection is crucial in sport and there are several ways that sports organisations could lose significant sums of money due to legal costs or regulatory fines upon any mishandling of personal and sensitive information. We see there is a need for good security hygiene at player and individual level, in terms of securing online social media accounts, and a need for protections of high-profile sportspeople who have a big online digital footprint. There is a strong duty in sport to protect fans, both digitally in terms of secure online payment systems for tickets and merchandise, but also in terms of safety and privacy where technologies such as smart turnstiles and CCTV are used at sports venues.



Cyber Threats and Attacker Motives in Sport

Expanding on the findings from our online literature review, we can summarise the key cyber threats in the world of sport, the likely threat actors and their motives.

Who or what	Motive	Methods	Potential Business Impact
Industrial or Rival Espionage	With sport being highly competitive by nature, examples of industrial espionage might include: • Obtaining secret team or player strategies. • Obtaining details about player purchases and loans during transfer seasons. • Theft of intellectual property (e.g., blueprints and designs of Formula 1 cars).	Targeted hacking against organisations or key individuals who would have access to the level of information sought (e.g., managers, CEOs, engineers etc.). Espionage techniques such as deployment of spying equipment (e.g., bugs, GPS trackers) or use of drones to spy on training sessions.	Such attacks can lead to the unauthorised disclosure of strategic plans, player health data, or team strategies, eroding a team's competitive edge. Moreover, the compromise of financial data can jeopardise sponsorships and revenue streams, while a tarnished reputation from a breach can alienate fans and stakeholders, ultimately threatening the financial stability and competitive standing of the organisation.
Organised Crime	Ransomware might be mounted against sports clubs or organisations to render them non-operational until they pay a ransom. This might also include a targeted data breach and threat to release sensitive data unless a ransom is paid. Match-fixing: obtaining relevant information to gain advantage in match-fixing or improving gambling success. Business / ticketing fraud: financial gain from fraudulent activities performed against organisation employees, fans or spectators.	Ransomware and data breach attacks will occur as a result of hacking of corporate IT systems, which may originate through targeted phishing attacks against organisation employees. For business fraud, attacks might also include eavesdropping and hacking of IT systems and phones of key staff. Ticketing fraud might exploit security weaknesses in online or mobile ticketing apps, or leverage mass deception with fake ticketing websites.	Potential significant financial losses from ransom demands, disruptions to ticket sales and merchandise operations. Moreover, unauthorised leaks of sensitive data can erode fan trust, damage brand reputation, and result in costly legal battles. Furthermore, an interruption to broadcasts or streaming services (pivotal revenue streams for many sports entities) can have lasting financial and reputational repercussions.

Who or what	Motive	Methods	Potential Business Impact
Hostile Nation States	Geopolitical motivations could include: • Wanting to discredit the reputation of a club, organisation or nation in the face of geopolitical tensions • Compromising the integrity of medical records to deceive or disrupt. • Targeted spying on sportspeople when they visit hostile states for sporting competitions. • Ransomware attacks: some hostile nation states may use ransomware as both a means to disrupt and obtain funds, often leveraging organised criminal groups to perform the hacking activities.	Network-based hacking, usually via targeted phishing attacks and often leveraging organised criminal groups for this activity. Exploitation of various forms of IT equipment (e.g., mobile phones, fitness trackers) to track and spy on persons of interest. Online propaganda and misinformation campaigns, leveraging social media bots and similar.	Hostile nation state actors may exploit vulnerabilities to manipulate game outcomes, access sensitive team strategies, disrupt live broadcasts, or even exploit fan data, in bids to undermine or discredit an organisation or entire country due to geopolitical tensions.
Insider Threat / Disgruntled employees	Financial gain could be a motive, either launching a ransomware attack from already privileged system access or performing some other form of electronic fraud against a club or organisation. There might also be a motive of reputational damage caused via a deliberate data breach and exposure.	This might not need any sophisticated technical skills if an employee already has access to sensitive systems and data. Coercion (threats or bribes) by organised crime or hostile nation states might be involved, leveraged to facilitate unauthorised access to IT systems in some way.	Might lead to the unauthorised disclosure of sensitive team strategies, personal athlete data, and financial information. This not only damages the organisation's reputation and competitive advantage but can also result in substantial financial losses due to legal repercussions, regulatory fines, and lost sponsorship or fan trust.
Cyber Bullies / Trolls	To cause distress and upset of sportspeople, leveraging harmful language and traits such as racism, homophobia and misogyny.	Mostly performed via social media (Twitter, Facebook, Instagram), often from anonymous, non-attributable online accounts.	The emotional and psychological toll on athletes can affect on-field performance, weakening team dynamics and potentially influence game outcomes.

Who or what	Motive	Methods	Potential Business Impact
Casual Attackers / Script Kiddies	Typically hack for fun and curiosity, but with potentially damaging outcomes such as public data breaches which they perform to gain a level of kudos and notoriety amongst their peers.	Use of general hacking tools and techniques, and not to be underestimated in terms of technical skill despite their likely young age.	Even low-skill attackers or "script kiddies" pose a genuine threat to sports organisations. Their use of readily available hacking tools can disrupt digital operations, lead to unauthorised data access, or cause public relations nightmares, all of which can result in financial losses, damaged reputations, and undermined fan trust. As the sports industry increasingly relies on digital platforms for fan engagement, ticketing, and operations, the business risks associated with even seemingly minor cyber intrusions should not be underestimated.
Hacktivists	To disrupt or discredit sportspeople, clubs, organisations or countries considering things such as controversial tournament hosting, controversial beliefs, attitudes towards equality etc.	Hacking, usually via targeted phishing to gain access to private emails or phone messages that if exposed publicly could cause significant controversy and reputational damage.	If targeted by hacktivists who oppose an organisation's values or beliefs, these entities can experience not only direct financial losses but also reputational damage, undermining fans' trust and corporate partnerships. The subsequent loss of consumer confidence, combined with potential regulatory penalties and the cost of rectifying breaches, can have long-term repercussions on a sports organisation's profitability and brand value.

Who or what	Motive	Methods	Potential Business Impact
Organised Gamblers	Illegally influencing sports outcomes for some level of betting advantage – e.g., to improve chances during in-play betting, or more broadly to affect entire outcomes of sporting events. Slightly different to organised crime in that the motive here is always about gaining advantage when betting, rather than monetising actual hacking activity such as ransomware.	Use of various technology methods to gain a gambling edge and/or influence sporting outcomes. Could be through use of drones or other monitoring equipment, or via hacking activity leading to physical control and disruption of systems such as pitch heating, floodlight or smart turnstile systems (perhaps to instigate a game postponement) or even wireless interfaces and control units in Formula 1 cars. Could also be as simple as bribing vulnerable or corruptible sportspeople and referees.	Organised gamblers might undermine the integrity of a sport, leading to compromised competitive outcomes, tarnished reputations, and significant financial losses. Such breaches may distort betting odds, manipulate game results, or leak sensitive data.

Key Themes, Findings & Observations

Our research sought to gain insights into existing cyber security practices or concerns within the sporting world through an anonymous online questionnaire issued to various people who work in the world of sport, and one-to-one interview sessions with IT and security managers tasked with securing their organisation – in the context of this report we use the term organisation to encapsulate a range of entities such as clubs, racing teams, sporting bodies etc. Despite the online questionnaire being completely anonymous and distributed to hundreds of people working in the world of sport, the number of responses was minimal and not particularly insightful by way of quantitative statistics. As such, we instead focused gaining insight from the one-to-one interview sessions held with people working across a range of sports organisations – most interviews were performed with individuals working in the highest levels of professional sport, such as Premier League football in the UK and Formula 1 racing.

Sports organisations – findings from one-to-one interviews

Resource Constraints & Board Awareness

A common concern was voiced around limited IT and cyber security roles and headcount within sports organisations – apart from some examples in Formula 1 racing, there aren't typically Chief Information Security Officer (CISO) roles at sports organisations, unlike in most other sectors. It was also often reported that the same IT system management staff are also tasked with cyber security duties but with very limited financial resource available for security assurance activities.

Convincing boards to spend on cyber security was commonly reported to be difficult. Despite IT teams articulating various cyber security risks, sports organisation boards were often more prepared to accept risks than close any security gaps that would cost time and require human resource. As a result of these resource constraints, a low level of cyber security maturity exists in many sports organisations which is often at odds with the overall high-profile nature of those organisations – one such organisation (whose owners have a combined net worth of £billions) had less than 10 staff in IT and security departments combined, but were tasked with securing the multi-million-pound enterprise. The IT manager explained the dichotomy of an organisation that spends £millions on just one player, but where a £75,000 annual salary for a skilled cyber security professional is too prohibitive.

> *"Dealing with a football club is essentially dealing with two entities - you have the playing side which is a big business and then you have an SME on the other side running it with limited staff and budget"*- Football Club IT Manager

Lack of awareness of cyber security threats at board level was attributed to lack of cyber security resource commitment. A few examples were cited where it is commonly believed at board level that antivirus software and firewalls are all that is needed to defend against cyber attacks, demonstrating an outdated view on what exactly is needed to secure a modern enterprise across people, process and technology.

Overreliance and spend on cyber insurance

Many organisations reported that they take out annual cyber insurance, the premiums of which can be quite expensive and where the cost of those premiums would probably be better spent on implementing proactive cyber security controls and defences. A few organisations noted that the premiums for cyber insurance were rising almost exponentially each year, with insurance providers increasingly demanding more on cyber security maturity (such as active security testing and audits) to satisfy underwriters.

Some organisations were aware that while cyber insurance provides some level of financial protection in the wake of an incident, it doesn't protect against reputational damage, or severe impact on business operations – the main concern raised here was a potential ransomware attack against an organisation; should the organisation not pay the ransom, or the decryption mechanism for the ransomware not work for some reason, then any cover by insurance would be spent on rebuilding the entire infrastructure which could take months, while in the meantime the organisation would be unable to function properly and would no doubt be seeking to repair reputational damage from the inevitable public knowledge of the cyber attack.

No industry or peer benchmark

Sectors such as banking, healthcare and e-commerce have been more scrutinised over the years in terms of cyber security capability, largely facilitated through regulation, allowing for a clearer view on overall maturity and providing the ability for industry peers to benchmark themselves. No such industry or peer benchmarking exists for the sports sector, and this was raised by a few organisations as a general unknown for them. For example, are they spending enough on cyber security compared to their peers and other sectors? There's currently no yardstick on how much organisations should be spending on cyber security, commensurate with their size and position within leagues or divisions for example.

Also, regarding peer comparison, many organisations mentioned that they'd be open to sharing with other organisations (even across different sports) about their cyber security efforts and concerns. Many believed such a forum of knowledge and experience sharing would benefit the overall sports sector.

Keeping pace with the ever-evolving technology and threat landscapes

Almost every sector struggles to keep pace with the ever-evolving technology and threat landscapes, and this was particularly true for most sports organisations interviewed. In sport, these struggles are compounded in complexity and risk where clubs might experience sudden and rapid growth, such as promotion to a higher league and/or new club owners and investment – these sudden changes typically demand more technology and change, which becomes even more difficult to manage and assure from a security perspective with limited resource.

To manage fast pace of change and with limited resources, a few organisations noted their preference on outsourcing as many IT and security functions as possible, including increased use of cloud technologies to minimise maintenance requirements on-premises. However, this has created additional issues around lack of training on cloud technologies and managing security policies across cloud infrastructures. In addition, outsourcing may have increased risk due to lack of centralised governance and limited to no security due diligence performed on third parties.

Little to no third party due diligence in place

Despite high use of third parties across various sports organisations, most noted that their abilities to perform security due diligence on those third parties was limited to zero. Organisations in Formula 1 racing for example will typically have hundreds if not thousands of third party suppliers and partners, from manufacturers of nuts and bolts right up to race team sponsors. Knowing how to prioritise due diligence activities on large supplier lists was a common concern, with some taking the approach of performing more checks on the larger organisations, which may or may not be the best approach in terms of gaining overall security assurance in a large supplier network.

Ransomware is a huge concern

Ransomware is a huge concern for most sports organisations. Many reported that phishing attacks were the likely initial entry point into an organisation's network which might then result in a ransomware attack. Some organisations face the additional challenge of managing Bring Your Own Device (BYOD), where commonly staff on the coaching and management side will use their own laptops at training sessions and matches – these BYOD devices may not be properly secured yet may access and store sensitive organisational information, rendering them at risk of various cyber attack and/or data breach through lost or stolen laptops, phones and tablets.

Little to no cyber security governance or standards in place

Mature organisations in any sector will put in place policies and processes to govern the organisation's approach to securing networks, systems and data – commonly referred to as an Information Security Management System (ISMS). Various international standards (e.g., ISO-27001) and national security assessment schemes (e.g., Cyber Essentials) exist to support consistent and appraisable approaches to an ISMS.

Hardly any organisation interviewed had a robust ISMS in place. Some of the more mature organisations were cherry picking subsets from ISO-27001 deemed to be priority areas for them, while other organisations were being forced to demonstrate some level of ISMS as a condition of their cyber insurance policies. All organisations were conscious of the need to adopt a robust ISMS.

It was however apparent that organisations processing payment card data were very familiar with Payment Card Industry (PCI) standards and compliance and understood the importance of achieving and maintaining this compliance to protect customer card data.

Cyber training and awareness is light touch

Organisations were engaging in some form of cyber security training, however this mostly consisted of annual phishing exercises against staff and some limited Computer-Based Training (CBT) each year on some of the basics of cyber security hygiene. Despite some training and awareness, organisations admitted that employees would still fall victim to phishing exercises, including some who'd had several years of training from routine phishing exercises. It was acknowledged that while phishing exercises help to inform, educate and maintain awareness, the exercises in isolation won't stop some employees being deceived and thus additional security controls and processes are needed as part of defence-in-depth approaches to cyber security.

Conversing around this topic also revealed that most organisations have never engaged in any cyber attack simulation or desktop exercise around incidents and lack any processes or playbooks to follow in the wake of a cyberattack or incident.

A big challenge for many clubs is securing the C-Suite and Management layers – these tend to be the least compliant or educated in terms of cyber security hygiene, and yet are the most visible and exposed due to their regular media appearances.

Little to no incident response capability

Organisations had limited to no incident response capability, meaning that in the event of a ransomware attack, data breach or other type of cyber intrusion, they wouldn't know what process or procedure to follow, or even which third party incident response bodies or providers to contact for assistance.

Inconsistent approaches to Identity & Access Management (IAM)

Many interviewees expressed concern about their organisation's outdated approaches to IAM, specifically around use of passwords. Passwords used in isolation as an authentication factor are not in line with modern best practice, especially when those passwords might be weak in terms of their length and/or ability to be easily guessed (lack of complexity). Stronger approaches to authenticating users to networks and systems include Two-Factor Authentication (2FA), where additional factors such as something you have (e.g., a hardware or software token) and/or something you are (e.g., biometrics such as fingerprint or face recognition) are used in addition to passwords.

As a side activity during this research, NCC Group created a list of 107 generic email addresses relating to the twenty teams in the English Premier Football League. These email addresses were taken from each club's official website, typically relating to contact details for things like ticket enquiries, media enquiries and hospitality visits. Fictitious examples include tickets@footballclubname.com, media@footballclubname.com and events@footballclubname.com. These email addresses were then searched on the HaveIBeenPwned website, which allows for checking of the presence of email addresses in known and published data breaches. The results were surprising – mostly because registering accounts with other websites (in one example, an online gaming website) with generic email addresses is unusual (and risky). Many breaches were identified, meaning those email addresses, particularly if using shared passwords across club logins and with weak passwords, might be at risk of compromise.

> 60% of generic email addresses used by all Premier League Football Clubs have appeared in known public breaches. One club's email address appeared in 16 unique public data breaches. - NCC Group

Physical security and links with cyber security not understood

Modern sports venues are increasingly connected and technologically sophisticated. While this creates an enhanced experience for fans and streamlines operations, it also creates a wide potential attack surface. Over the past decade NCC Group has performed many security assessments of sports venues, ranging from physical security through to network security of the various connected devices used in modern sports venues to facilitate business operations, fan experience and safe environments for spectators.

Commonly, but often unknowingly, many stadium-based systems are connected to corporate networks of sports organisations. Examples include public address (PA) systems, automated lighting controls (smart floodlights), point of sale (PoS) systems for food and drink vendors, CCTV and facial recognition systems, or heating, ventilation and air conditioning (HVAC), to name but a few. In addition, many stadiums and sports venues have adjoining hotels and hospitality venues, which often share and bridge the same Wi-Fi networks with organisation corporate networks. The potential attack surface against a modern connected stadium is therefore vast, and likely comprising disparate yet interconnected systems of many third parties and in varying states of security configuration.

Our interviews with various sports organisation IT managers revealed either known concerns about this level of connectivity, or lack of awareness about the potential interconnectivity of so many systems due to a high-level of outsourcing of IT and connected stadium functions.

From a physical security perspective, historically, NCC Group has successfully breached various venue physical security controls from electronic bypass of vulnerable door entry controls, through to more socially engineered approaches such as masquerading as tradespeople. Other successful physical to electronic intrusions have previously involved attending an official stadium tour but straying away from the group at opportune moments to then access meeting rooms with open network ports allowing for onward network-based intrusion attempts.

Some interviewees were aware of the UK's plans for new laws (Martyn's Law) to protect against terrorism in public places, inclusive of sports venues and high-capacity locations. For some venues, this will require enhanced physical and electronic security controls (budgets for which may not exist) – concerns were expressed around potential liability in the event of a physical or cyber breach that might subsequently lead to a terrorist attack against a venue.

Data Protection in Sport

Several organisations raised concerns about the huge volumes of data that they generate, process and store, ranging from financial data through to sensitive health and medical records of sportspeople. Organisations typically don't perform any data mapping exercises to understand where all their data assets are stored and processed (and by whom) – this causes concern not just because of the potential for data breach by hostile attackers, but also a general (perhaps unintentional) mishandling of data by club employees, such as lost or stolen IT assets, or accidental emailing or publication of sensitive information.

As part of this research NCC Group performed an online survey of sports-related data breaches that had resulted in financial and regulatory fines under the General Data Protection Regulation (GDPR).

Who was fined?	Why?	Fine
The Royal Dutch Tennis Association ("KNLTB"), Netherlands	Selling the personal data of more than 350,000 of its members to sponsors.	€525,000
National Football League (LaLiga), Spain	Failed to inform users of the implications contained within an app it offered users - the app remotely accessed the users' microphones once every minute to check pubs screening football matches.	€250,000
Club Gimnasia Ritmica San Antonio, Spain	The data controller had posted pictures and videos of the complainant's two underage daughters on Instagram, despite the complainant's prior non-consent instruction.	€5,000
VfB Stuttgart 1893 AG, Germany	The football club was fined for a negligent breach of data protection accountability.	€300,000
Apoel FC, Cyprus	Because of a lack of security measures in the football club's ticket sales system, unauthorised individuals could access personal data of fans visiting the club's website.	€40,000
UAB VS FITNESS, Lithuania	The consent provided by the customers to have their fingerprint scanned was not voluntary since no other identification measures were in place. Moreover, the DPA discovered that the data controller also illegally processed its employees' fingerprints.	€20,000

Some of the data breaches listed also show procedural issues concerning data handling, and/or lack of awareness of what type of data is not appropriate to publish or share without proper consent. This is particularly concerning in the world of sport which, more than other sectors, commonly processes data of children who start their sporting careers early and can even sometimes perform professionally as minors. The fines (one of which was over half a million Euros) demonstrate the potentially severe financial penalties for mishandling data; funds that might otherwise have been spent on training, awareness and proactive security controls and defences.

Other areas of note or concern raised by interviewees

In closing our one-to-one interviews, we asked interviewees if they had anything else they'd like to raise or mention by way of thoughts, issues or concerns. Key areas raised by two or more individuals included:

- There's no cyber security regulator or assurance scheme specific to sport – while some sectors have specific cyber security regulations and assessments, such as CBEST threat intelligence-led assessments in financial services, there is currently no equivalent in sport, meaning there are no drivers to support baselining and then improving the maturity of sports organisations at a regulatory level

- A few organisations within the same sport felt that the parent or governing body of that sport could take more of a lead on provision of cyber security advice and guidance to ensure consistent, minimum-security standards across organisations. In addition, this could include wholesale buy-in of cyber security products and services to achieve economies of scale and to facilitate a common approach to cyber security across organisations

- Rival espionage is real – while not necessarily always a cyber-threat, a few organisations mentioned the value of the data that they hold, from drone footage at player training sessions through to Formula 1 car performance data. Rival teams might endeavor to obtain this information for their own advantage. A few clubs mentioned that they perform routine bug sweeps of their premises due to their concerns in this area

- The insider threat is likely highly overlooked in the world of football – concerns were raised regarding staff vetting (just minimal DBS checks) – this includes everyone from IT staff through to match security workers. Again, lack of budget and resources were attributed to only the bare minimum checks occurring in professional football for example

Sportspeople Security

Our research also investigated cyber security concerning sportspeople at an individual level. In professional sport many sportspeople can be high-earning, high net-worth, individuals amassing wealth from salary, bonuses, transfers, sponsorship deals and, where applicable, tournament prize money. As such this renders professional sportspeople at risk of several potential security issues.

Targeting by organised crime, organised gambling or industrial espionage

Many threat actors may have motives to learn about a sportsperson's training programmes, injuries, health information or private emails between coaches, doctors, accountants and sponsors to gain some level of competitive advantage when betting, or to extort a sportsperson for some financial gain. Sportspeople may therefore be targeted through spear phishing or similar in attempts at gaining unauthorised access to their IT systems.

High use of connected technology

High-earning sportspeople will use a lot of connected technology beyond just laptops and computers. Examples include fitness trackers and other connected health devices, possible use of high-end cars (the modern vehicle being connected in several different ways) and likely increased use of Internet of Things (IoT) and security systems at their homes. All these connected devices increase the potential attack surface against individuals.

Large online digital footprints

High-profile sportspeople typically have large digital footprints due to their use of social media platforms and applications. Even if social media isn't directly used by them, they may allow access to their management teams to publish content on their behalf. This can expose sportspeople to several potential issues including cyberstalking (revelations about their whereabouts and GPS coordinates can be used to track where they are) and cyber bullying – According to a research paper, bullying is acknowledged by scientists as a considerable and still unresolved problem in sport. By triggering stress-related emotions through bullying, this causes various negative effects on physical and mental health, which consequently will affect performance during play. Use of social media also increases the risk of account hijack, which if successful could be used by attackers to publish something offensive but purporting to be written by the victim, in bids to damage the reputation of a sportsperson for example.

Our research identified that sports organisations and clubs need to train and educate sportspeople on good cyber security hygiene and practices, beyond just training their IT and office staff. In addition, there is a likely broader need for provision of mental and emotional support to sportspeople who are victims of online abuse.

Fan and Spectator Security

The main cyber threats to fans and spectators are financial fraud relating to tickets, privacy impacts due to any personal data breaches and physical safety at sporting events where there may be cyber-physical systems such as smart turnstiles.

Ticketing Fraud

Ticketing fraud is a major issue for sport and can occur in different ways:

- Legitimate ticket sites might be hacked and malicious software injected into the website which steals credit card information of victims when purchasing tickets
- Fake yet convincing ticket sites can be created by cybercriminals, and victims lured to these sites through phishing attacks or social media deception – the sites purport to be selling tickets and consume victim payment card

> In 2022, data revealed a 68% rise in football ticket scams between January and June, with an average loss of £410 per victim - Lloyds Bank

Most interviewees in our research felt that their organisations were quite aware of PCI compliance obligations and its importance in relation to securing payment data of fans, but those organisations weren't necessarily performing routine security tests or checks of their ticketing websites. Organisations felt less in control over the broader issue of fake or scam ticketing sites, acknowledging that it would be good to issue regular guidance to fans to minimise their chances of falling victim to ticketing fraud. Some guidance is available from the Premier football league for example.

While not necessarily a cyber security issue, a few organisations mentioned the related issue of fake merchandise and how that can severely impact merchandise revenue.

New approaches are currently being explored to combat ticket fraud, including use of blockchain technologies and digital tickets to block ticket resale and remove the need for physical tickets. Such technologies, however, may bring with them new forms of potential attack or subversion.

Privacy and data protection

Organisations may capture personal information of fans – common examples will include payment card data for tickets or food and drink at stadiums, names, email addresses and dates of birth of supporters for mailing lists and possibly facial imagery from CCTV systems at stadiums.

Organisations therefore have obligations on securing these sources of data in line with data protection regulations such as GDPR. In 2018, Liverpool FC confirmed that personal details of season ticket holders (including home address and bank details) had been exposed, because of a staff email account being hacked by a malicious third party.

Facial recognition is increasingly being used at stadiums for:

- Detecting known troublemakers, criminals or terror suspects
- Improvements in fan experience through automated access control and personalised entry experience

Fans and spectators will require assurances around the secure handling of any of their biometrics captured at sports venues, while GDPR and similar data protection obligations on sports venues that capture biometrics will include:

- Transparency: Sports venues are generally required to inform visitors if their biometric data is being collected and for what purpose
- Purpose Limitation: The data collected should only be used for the purpose specified and nothing else
- Data Minimisation: Only the minimum amount of data required for the task should be collected
- Signage: Clear signage must be displayed notifying visitors that CCTV or other surveillance technology is in operation
- Consent: In some cases, explicit consent might be needed to collect sensitive personal data, which includes biometric data
- Data Protection Impact Assessment (DPIA): For technologies with high potential impact on individual rights, such as facial recognition, a DPIA may be required

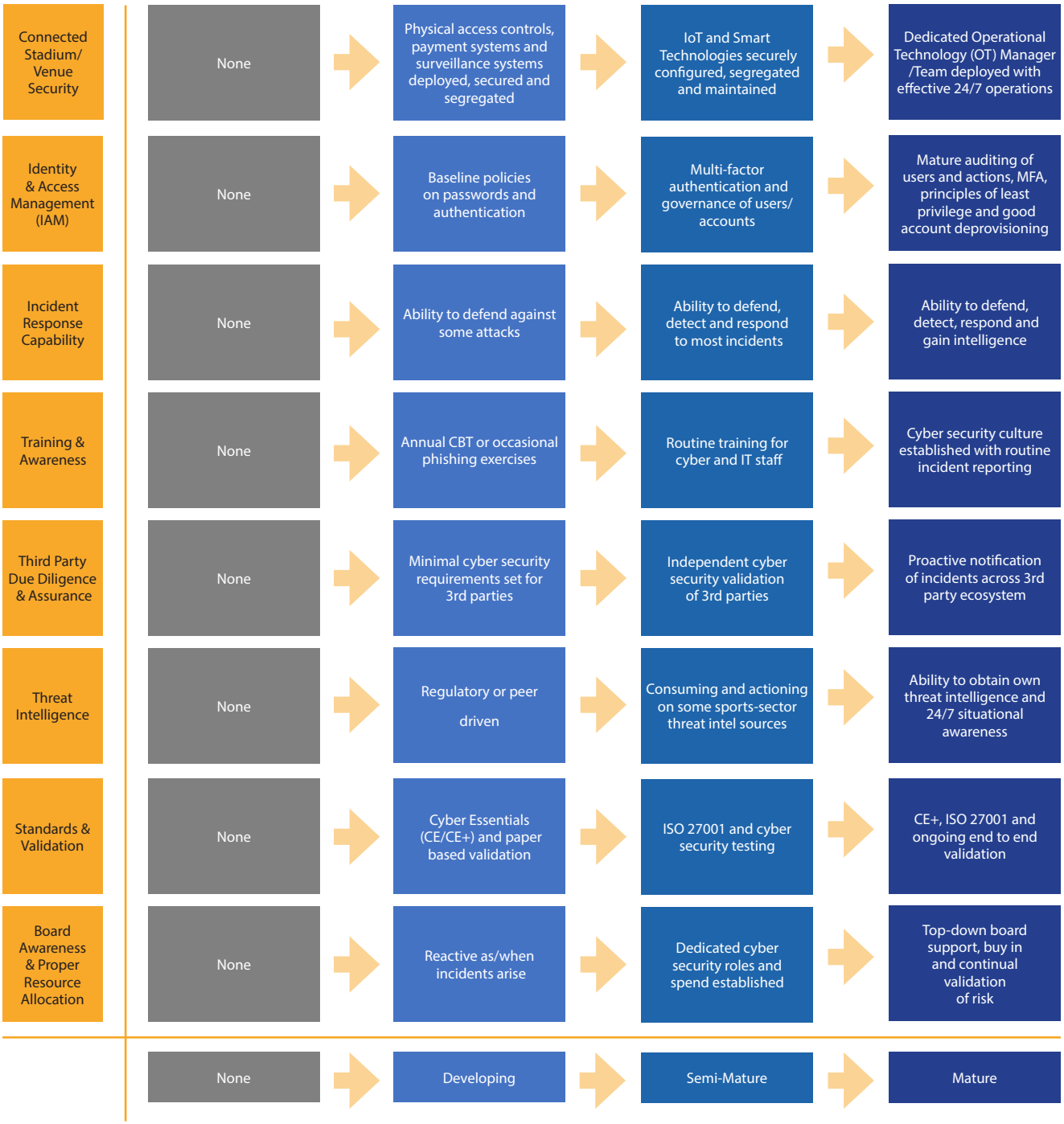
Safety and physical security

Physical safety surfaced several times as a topic during our research. With evermore connected stadiums and use of cyber-physical systems such as smart turnstiles or even moving pitch technology, these systems present potential for physical harm if they fail or are disrupted through cyberattack.

One can imagine horrific, yet believable scenarios where everything is connected and thus potentially accessible to attackers; without proper network segregation and security controls, conceivably an attacker could disrupt a well-attended night-time game by locking smart turnstiles, turning off the floodlights and then enabling the fire alarm – this could invoke a stampede with poor visibility and could cause serious harm or even loss of life. While these are awful scenarios, they are legitimate scenarios that need be played out as part of threat modelling of connected stadiums, and how/where the health and safety of spectators could be affected because of a cyber attack against a connected stadium.

Cyber maturity in sport – how to improve cyber security posture

In concluding our research, we present a cyber security maturity model for sports organisations. The model is derived from the key themes and concerns raised during the research by sports organisations, sportspeople and sports fans and spectators – it sets out the various security assurance activities that sports organisations should perform to progress through to higher levels of maturity, minimising risk and exposure during that journey. The model is a guide rather than an absolute, but if followed should help sports organisations benchmark where they currently are in terms of cyber maturity, where current gaps in key areas may exist, and to look at where they want to be, or can best be within specific budgetary and resource constraints.



Prioritising cyber security spend

A common theme from our research surfaced around cyber security spend in sport, and what should be considered adequate budget depending on the size of a sports organisation. This is always a difficult question to answer in any sector, and there certainly isn't an agreed standard budgetary range for cyber security spend since different organisations will have different technology stacks, sizes and capabilities of security teams, different levels of threat and risk etc.

It is possible however to provide some level of guidance on cyber security spend, commensurate with an organisation's size (in terms of turnover and number of employees), and the level of cyber security maturity that the organisation is seeking to achieve. The following suggested percentage of spend of annual turnover, commensurate with organisational size and intended level of cyber security maturity provides some guide on what might be deemed adequate:

Size	Immature	Developing	Semi-Mature	Mature
Small	Up to 1%	Between 1% & 2%	Between 2% & 5%	5% or more
Medium	Up to 2%	Between 2% & 3%	Between 3% & 7%	7% or more
Large	Up to 3%	Between 3% & 5%	Between 5% & 10%	10% or more

Again, we reiterate that there's no science behind these recommended figures, but rather they provide a general, average indication of how much sports organisations might typically expect to be spending commensurate with their size and cyber security maturity goals. For some organisations, the suggested levels of cyber security spend may seem excessive, and/or concerns may exist about what the spend is achieving – another common theme from our research interviews was how in the world of sport, it can be hard to comprehend what the value is of a cyber security product or service.

An example was given from professional football, whereby when a player is bought through a high value contract, it's easy to see the ROI of that player based on their performance at each match throughout the season. A few interviewees reported how at board level, there is often pushback on cyber security spend since it's not easy to visualise or conceptualise exactly what a cyber security product or service is doing, particularly since cyber attacks are ephemeral and ethereal in nature. The main issue with this type of perspective is that organisations will be unprepared and become reactive to cyber incidents and attacks, often (or mostly) when it's too late. In a very recent Cost of Data Breach report from IBM, the global average cost of a data breach in 2023 was $4.45m USD. With any additional financial impact of ransomware payments or legal and regulatory fines, these figures suddenly make more sense to be spent as proactive, defensive measures through cyber security products and services.

A note on getting the basics right

The importance of fundamental cyber security measures and effective lifecycle management in professional sport cannot be overstated, especially when communicating these necessities to decision-makers at board level. Often, the foundational elements of cyber security - such as regular software updates and consistent patching, get overshadowed by more complex, cutting-edge solutions. Yet, it's these basic measures that form the bedrock of a secure digital environment.

While foundational, these processes can admittedly be challenging to implement and maintain. They are time-intensive, can appear monotonous, and may not yield immediate, tangible results. The paradox lies in the fact that when these tasks are executed effectively, they operate in the background, often going unnoticed. However, their absence or mishandling can lead to significant vulnerabilities and subsequent disruptions.

Furthermore, the implementation of these basic measures such as software updates, can occasionally cause temporary outages or unexpected operational impacts. Such disruptions can place additional burdens on system administrators and IT teams. Yet, this highlights the very reason why the commitment to cybersecurity needs to be organisation-wide. It's crucial for board members and senior leadership to recognise the value of these foundational security practices. By doing so, they provide the necessary support and resources that allow technical teams to carry out their responsibilities effectively, ensuring the organisation's cyber resilience in the face of growing threats.

Conclusion

This research yielded valuable insight into the cyber security threats that face the world of sport, and what the sports sector can do to improve its overall cyber security maturity to better secure its organisations, employees, sportspeople, fans and spectators. Compared to other sectors (particularly those sectors that are highly regulated), the sports sector appears to be at much earlier stages of cyber maturity, struggling to maintain pace with the ever-evolving technology and threat landscape and the dynamic nature of change in sport in general (when key events such as league promotions or new owner acquisitions occur). The sports sector is therefore at higher risk of cyber attack and incidents than other sectors.

Interviewees were deeply concerned about several potential cyber threats against their organisations and what the resulting financial and reputational damage could be following any real world cyber incident. Thes concerns included ransomware attacks, attacks against connected stadiums and venues and the potential impact on player and spectator safety, insider threat due to limited vetting procedures and even rival espionage, performed via cyber-borne activities.

Despite the myriad of concerns by employees working in IT and security departments within sports organisations, the key theme that surfaced from research interviews was a lack of awareness of cyber security at board level, and the need for proper cyber security investment to defend and mitigate many forms of cyber threat. In NCC Group's experience, any successful cyber security programme of work and effective cyber security culture within an organisation, is driven top-down from board level, with comprehensive support and budget for people, training, technology and cyber security services. As such our research highlighted the need for increased board awareness and training around cyber security threats, and education on why cyber security maturity is paramount for protecting sports organisations.

Possibly related to limited board situational awareness was a general lack of cyber security governance within sports organisations. Many sports organisations feel they are still more reactive than proactive in their cyber security activities and would prefer to be working to a more defined governance structure.

In the absence of a cyber or security-focused regulator for sport, many interviewees expressed a willingness to openly share their experiences and insights from their cyber security efforts with others in the sector. Many believed such a forum of knowledge; threat intelligence and experience sharing would benefit the overall sports sector.
Most organisations expressed concerns around their limited capabilities in cyber incident response and third party security due diligence, highlighting a need for more support around these activities either within organisations through dedicated resource, and/or utilising professional cyber security services that can support 24/7 incident management and independent third party assurance checks.

Outside of organisational concerns, some noted the large online digital footprints of high-profile sportspeople, and how because of their large online presence, they might be exposed to various cyber threats including social media account hijacking, cyber bullying and general email account/laptop compromise in attempts to obtain sensitive, personal health and/or financial information. As such some felt that sports organisations may have a cyber duty of care for their sportspeople, and that suitable training and guidance should be provided to sportspeople to help them be safe and secure online.

The security and safety of fans and spectators also needs to fall within the remit of sports organisations. Clubs need to honour data protection legislation obligations for any personal data collected on fans and spectators, while their physical safety needs to be assured when stadiums and sports venues operate cyber-physical systems that if compromised, could result in physical harm or worst-case loss of life.

Ticketing fraud was also noted as a growing issue and concern – while sports organisations can do some things (mostly user awareness) around fake and fraudulent ticketing sites, much of this fraudulent activity is beyond the control of sports organisations meaning there is a need to lean on the capabilities of cyber-crime authorities to help minimise risk of fraud to sports fans and spectators.

Ultimately, it became clear that sports entities require assistance in determining how and where to focus their cyber security efforts and activities. They also need advice on setting benchmarks for cyber security maturity and enhancing it through greater investment and support. While the cyber security maturity model outlined in this report is at a high level, it should enable organisations to evaluate their current state of maturity. This, in turn, will help them identify their target level of cyber security maturity, thereby informing them of the necessary steps (and potential costs) to reach their optimal level of cyber security which will in turn, minimise risk and exposure to cyber attack and incidents.

Guidance and further resources

Board Awareness

- Cyber threat in sport: NCSC insight and guidance
- NCSC Board Toolkit

Early Warning

- Helps organisations investigate cyber-attacks on their network by notifying them of malicious activity that has been detected in information feeds

Cyber Security Standards, Testing & Validation

- Cyber Essentials – A government backed certification scheme that helps organisations guard against the most common cyber threats and demonstrate their commitment to cyber security
- NCC Group Cyber Security Review (CSR)
- DMARC (Domain-based Message Authentication Reporting and Conformance) - allows organisations to set a policy for how receiving email servers should handle emails, including untrusted emails which should be discarded
- Email security check - Free instant email security check
- Check Your Cyber Security - A free government service to help UK organisations check for cyber vulnerabilities
- NCC Group services on standards and compliance
- NCC Group security assurance and advisory services

Third Party Due Diligence & Assurance

- NCC Group supply chain and risk management services

Training & Awareness

- NCC Group technical training
- Phoenix Sport & Media Group Cyber Stars

Incident Response Capability

- NCC Group incident response services
- Exercise in a Box (EiaB)

Managed Security Services

- NCC Group Managed Detection & Response (MDR)
- NCC Group Managed Vulnerability Scanning Services (MVSS)

Connected Stadium / Venue Security

- CISA guidance on stadium security
- UK Sports Grounds Safety Authority Guide to Safety at Sports Grounds 'Green Guide'
- UK Sports Grounds Safety Authority Cyber Security for Major Events Guidance
- United Nations Office of Counterterrorism Guide on the Security of Major Sporting Events

Acknowledgements

We thank the following authors and contributors to this research and report:

NCC Group
Matt Lewis, Global Head of Research
Jon Renshaw, Deputy Director for Commercial Research
Verona Hulse, UK Head of Public Affairs

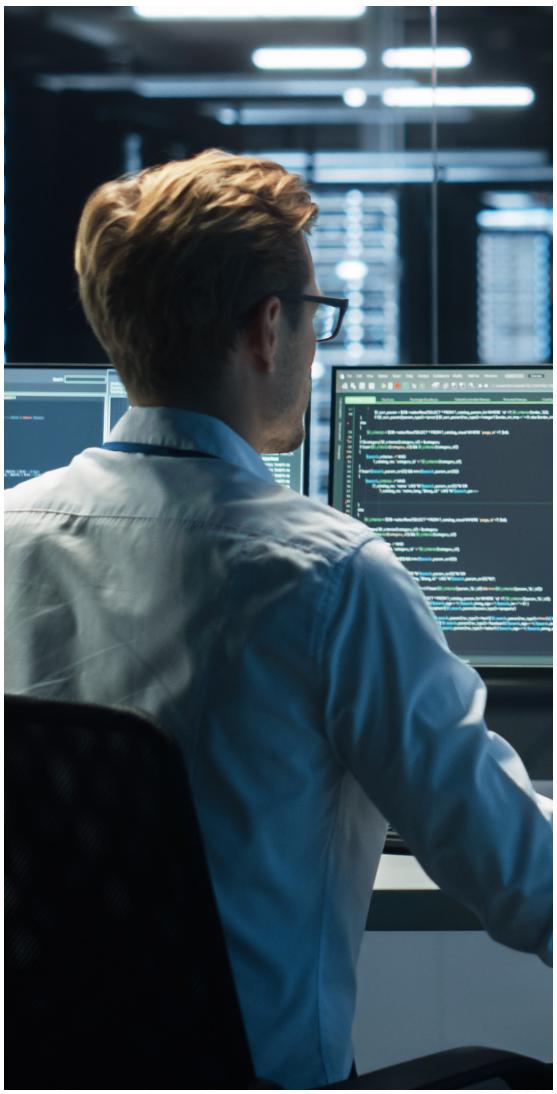
Phoenix Sports and Media Group
Carly Barnes, CEO

Phoenix Sports and Media Group provide cyber security training to sports organisations delivered by military veterans and tailored to meet the needs of sports organisations. Programmes are delivered to staff and players to ensure they have the skills required to identify an attack. PSMG's cyber awareness training is engaging and informative to ensure staff understand what is required of them and the importance of their role in safeguarding an organisation's sensitive data.

University of Oxford / Researcher Strategy Consultancy
Joseph Blayney
Kaustav Dey
Florian Groelly
Shuhan Jiang
Yangmei Li
Anna Tslapatanis

The Researcher Strategy Consultancy (RSC) programme provides early career researchers with an opportunity to develop the core employability skills required for a transition into analytical, business, or policy roles in a range of sectors.

Particular emphasis is given to business awareness, teamwork, communication and leadership to complement other training available to researchers. This programme enables participants to build on skills that typically develop in designing, planning and conducting complex research projects.



About us

People powered, tech-enabled, Cyber Security

NCC Group is a global cyber business, operating across multiple sectors and geographies.

We're a research-led organisation, recognised for our technical depth and breadth; combining insight, innovation, and intelligence to create maximum value for our customers.

As society's dependence on connectivity and the associated technologies increases, we help organisations to assess, develop and manage their cyber resilience posture to confidently take advantage of the opportunities that sustain their business growth.

With over 2,400 colleagues, we have a significant market presence in the UK, Europe and North America, and a growing footprint in Asia Pacific.

Contact Us:
cyberinsport@nccgroup.com
+44 (0) 161 209 5200
www.nccgroup.com

XYZ Building
2 Hardman Boulevard
Spinningfields
Manchester