Cyberfort

Case Study

How Cyberfort enabled a top tier Premier League Football Club to enhance its Cyber Security and Data Privacy capabilities.

Industry:
Sports
& entertainment

Location:
United Kingdom

A top-tier Premier League football club embarked on an ambitious digital transformation programme across its stadium, hospitality venues, and adjoining hotel infrastructure. As operations became increasingly interconnected and reliant on digital systems, leadership recognised the urgent need to enhance its cybersecurity and data privacy capabilities.

01304 814800 | cyberfortgroup.com | info@cyberfortgroup.com

Cyberfort

A top-tier Premier League football club embarked on an ambitious digital transformation programme across its stadium, hospitality venues, and adjoining hotel infrastructure. As operations became increasingly interconnected and reliant on digital systems, leadership recognised the urgent need to enhance its cybersecurity and data privacy capabilities.

With only foundational IT controls in place, there was no overarching cyber security strategy or data governance framework. Key challenges included:

- Limited visibility into data flows for players, employees, and guests.
- Fragmented asset management and risk ownership across departments.
- A growing reliance on third-party vendors and smart infrastructure (e.g., IoT systems in the stadium and hotel).
- Lack of alignment with leading security standards such as ISO/IEC 27001, 27701 and 22301.

The club needed a cohesive cyber security roadmap to support operational resilience, regulatory compliance (e.g., GDPR), and to uphold the brand integrity of a high-profile football institution.

Solution

A comprehensive cyber security strategy and roadmap were developed over a multi-phase programme, structured around discovery, design, and implementation planning. The following activities were undertaken:

1. Discovery and Stakeholder Engagement

- Conducted interviews and workshops with key stakeholders across IT, stadium operations, hospitality, HR, commercial, and the football department.
- Reviewed existing security controls, supplier security terms, incident response plans, and audit reports.
- Performed technical and process-based risk assessments across critical systems (e.g., ticketing, access control, hospitality management, and player analytic platforms).

2. Data Journey Mapping

Developed end-to-end data maps capturing the lifecycle of personal and sensitive data across:

- Player journeys (medical, biometric, performance, transfer-related).
- Employee journeys (recruitment, payroll, facility access, corporate systems).
- Guest and fan interactions (ticketing, Wi-Fi, hotel booking, loyalty and digital engagement).
- Identified systems, data processors, and third-party integrations that processed personal data across these domains.

3. Asset and Risk Management

- Delivered a full asset inventory and risk classification matrix.
- Introduced a tailored risk methodology that factored in business impact, regulatory exposure, and threat likelihood.
- Highlighted “crown jewel” assets and associated high-risk data flows, such as match-day broadcasting systems and VIP hospitality records.

4. ISO Framework Alignment

- Assessed the current control environment against ISO/IEC 27001 (information Security Management) and ISO/IEC 27701 (Privacy Information Management).
- Mapped gaps and defined a prioritised control uplift plan across 14 domains (e.g., access control, supplier relationships, incident response, and data subject rights management).

Business and Technology Outcomes

The engagement delivered a clear and actionable cybersecurity strategy aligned to the club's digital ambitions and stakeholder expectations. Key deliverables and outcomes included:

- **Cybersecurity & Privacy Strategy:** A five-year vision aligned with the club's growth across stadium technology, smart hospitality, and fan digital experiences.
- **Maturity Roadmap:** A phased improvement plan built around people, process, and technology, focused on increasing maturity across key domains (initial maturity score of 2.1 increased to a target of 3.8 over 18 months).
- **Data Flow Diagrams & Data Protection Impact Assessments (DPIAs):** Supporting GDPR compliance and supplier due diligence for systems handling guest and player data.
- **Risk Register & Asset Catalogue:** Foundation established for continuous risk monitoring and executive reporting, including integration into board-level risk reviews.
- **ISO Alignment Action Plan:** Practical, department-specific steps to work towards ISO/IEC 27001, 27701 and 22301 certification-readiness.
- **Executive Engagement & Governance Cadence:** Established a monthly cyber steering forum, integrating IT, security, legal, and operations to ensure ongoing accountability.

The outcome positioned the football club as a security-conscious, privacy-responsible organisation, fit for continued digital growth, partner confidence, and fan trust both on and off the pitch.