The Hidden Opponent: Cyber Threats in Sport

The global sports industry, projected to generate over $700 billion in 2026, is becoming an appealing target for cyber criminals due to its vast revenues and rapid digital transformation. From health monitoring technologies for athletes to the integration of smart technology in stadiums, the industry's expanding digital footprint increases its vulnerability to cyber attacks like ransomware, data breaches, and even threats to physical safety. Many sports entities lack the expertise and resources to counteract these threats. The world of sport has a pressing need for heightened cyber security awareness and proactive measures to ensure the safety and longevity of the sports sector in our increasingly connected, digital world.

Resource Constraints & Board Awareness

Sports organisations often face severe constraints in IT and cybersecurity resources, with many lacking dedicated Chief Information Security Officer (CISO) roles seen in other sectors. While the same IT staff manage system and cyber security, financial constraints limit their activities. Boards of these organisations are reluctant to allocate funds for cyber security, even when risks are communicated. This results in a stark contrast between the high-profile nature of these organisations and their low cyber security maturity. A common view at the board level in many sports organisations is that basic antivirus software and firewalls are adequate for defence, highlighting a dated understanding of modern security needs.

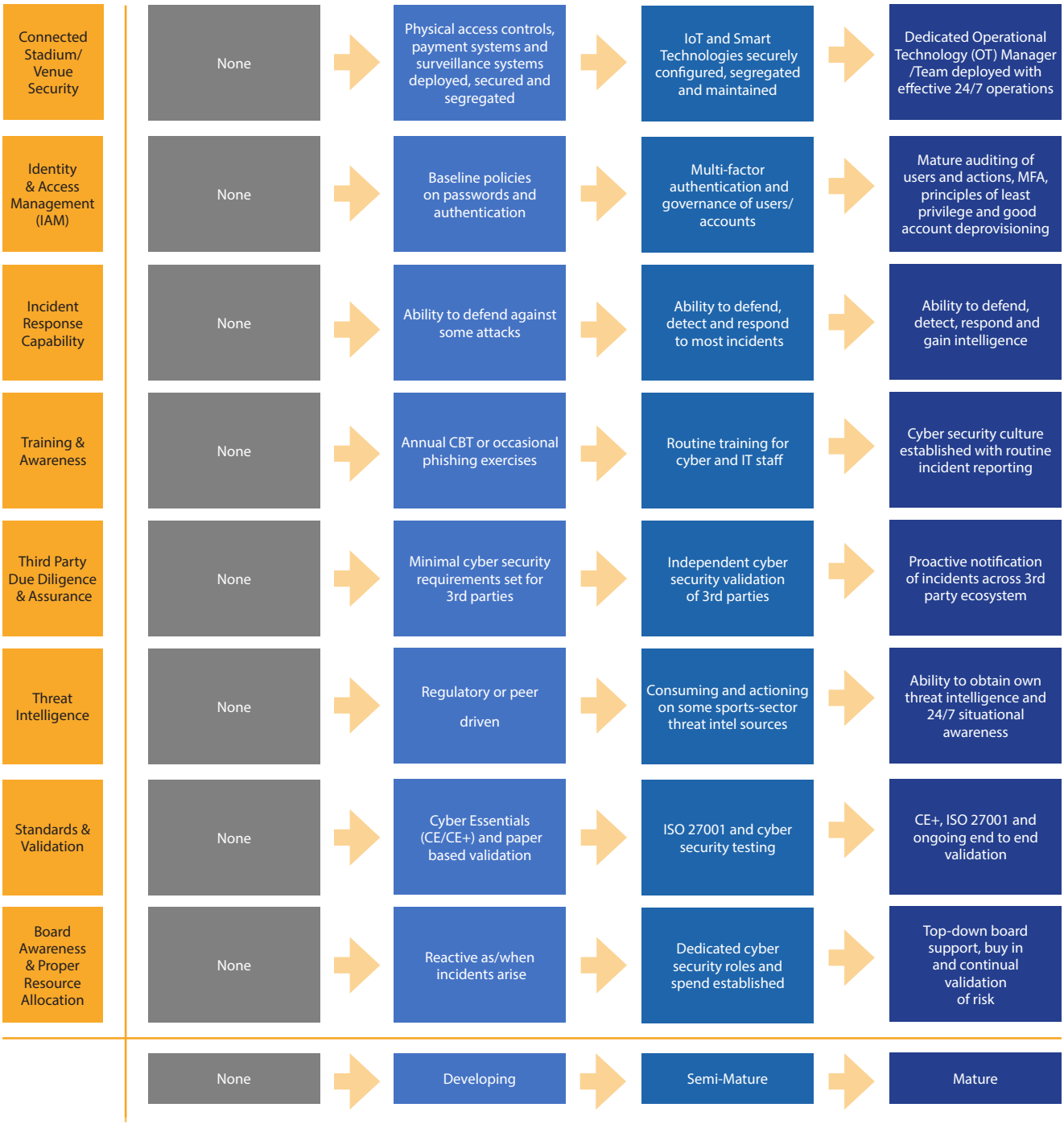
"Dealing with a football club is essentially dealing with two entities - you have the playing side which is a big business and then you have an SME on the other side running it with limited staff and budget"- Football Club IT Manager

Limited Spend

A challenge in the sports sector is justifying cyber security expenses, as it is hard to quantify the value of cyber products and services in contrast to tangible investments like buying players. Some boards struggle to conceptualise the benefits of cyber security, making them more reactive to cyber incidents than proactive. Given that the 2023 average cost of a data breach was $4.45 million USD (not counting potential ransomware payments or fines), investing in proactive cyber security measures is vital.

Cyber Maturity in Sport: How to Improve Cyber Security Posture

The sports organisation cyber security maturity model is derived from key cyber security themes and concerns raised by sports organisations. 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.


Connected Stadium/ Venue Security
None
Physical access controls, payment systems and surveillance systems deployed, secured and segregated
IoT and Smart Technologies securely configured, segregated and maintained
Dedicated Operational Technology (OT) Manager /Team deployed with effective 24/7 operations
Identity & Access Management (IAM)
None
Baseline policies on passwords and authentication
Multi-factor authentication and governance of users/ accounts
Mature auditing of users and actions, MFA, principles of least privilege and good account deprovisioning
Incident Response Capability
None
Ability to defend against some attacks
Ability to defend, detect and respond to most incidents
Ability to defend, detect, respond and gain intelligence
Training & Awareness
None
Annual CBT or occasional phishing exercises
Routine training for cyber and IT staff
Cyber security culture established with routine incident reporting
Third Party Due Diligence & Assurance
None
Minimal cyber security requirements set for 3rd parties
Independent cyber security validation of 3rd parties
Proactive notification of incidents across 3rd party ecosystem
Threat Intelligence
None
Regulatory or peer driven
Consuming and actioning on some sports-sector threat intel sources
Ability to obtain own threat intelligence and 24/7 situational awareness
Standards & Validation
None
Cyber Essentials (CE/CE+) and paper based validation
ISO 27001 and cyber security testing
CE+, ISO 27001 and ongoing end to end validation
Board Awareness & Proper Resource Allocation
None
Reactive as/when incidents arise
Dedicated cyber security roles and spend established
Top-down board support, buy in and continual validation of risk
None
Developing
Semi-Mature
Mature

Top 10 Recommendations for Sports Organisations

- Resource Constraints & Board Awareness: A major issue is limited IT and cyber security staffing. Sports organisations need to emphasise the importance of cyber security at the board level and ensure adequate budget allocation to counter risks effectively.

- Overreliance on Cyber Insurance: While insurance is important, clubs should be careful not to overlook implementing proactive cyber security measures. Reliance on cyber insurance alone will not prevent cyber attacks or protect the organisation's reputation in the wake of a cyber attack.

- Industry Benchmarking: Sports organisations lack a standard benchmark for cyber security practices, unlike sectors such as banking and healthcare. This makes it difficult for sports entities to evaluate their own security maturity relative to peers. Collaboration and networking with industry peers is key.

- Evolution of Technology and Threat Landscapes: Rapid technological advancements and growth (such as club promotion) can challenge a sports organisation's security infrastructure. There is a need for continuous assessment and adaptation to manage these challenges.

- Third Party Due Diligence: With many clubs relying on third party suppliers and partners, comprehensive security checks on these third parties are essential. Establishing clear criteria for security assurance among suppliers can mitigate potential vulnerabilities.

- Ransomware Concerns: The fear of ransomware in the world of sport, especially via phishing attacks, is significant. Protecting against these attacks requires comprehensive defences, including ensuring secure practices in BYOD (Bring Your Own Device) environments.

- Cyber Security Governance & Standards: Implementing recognised cyber security governance structures, like an Information Security Management System (ISMS), is essential. Adhering to international standards, such as ISO-27001, can guide these efforts.

- Training and Awareness: Clubs need more intensive and frequent cyber security training for staff. This should include simulations of cyber attacks to prepare staff for real world scenarios and heighten awareness, especially at the top management levels.

- Incident Response Capability: Organisations must be prepared with procedures and quick access to qualified third party support in the event of security breaches. Having an incident response plan and frequently testing security controls is crucial.

- Integrated Physical and Cyber Security: The integration of physical and cyber security in sports venues, given their technological sophistication, is vital. Understanding and securing all connected systems, including those of third parties, is paramount to reducing vulnerability and risk.

Sports organisations 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. Following a cyber security maturity model should enable sports 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.