Pulse Survey: February 2026

The Risk Landscape in Sport

HaysMac

Introduction

Tom Wilson
Partner, Head of Sport
T: +44 20 7969 5697
E: twilson@haysmac.com

As digital transformation accelerates across the sports sector, organisations are facing an increasingly complex risk environment. Cybersecurity threats, artificial intelligence adoption, regulatory scrutiny and economic pressure are no longer discrete challenges; they are converging in ways that amplify both operational and reputational exposure. At the same time, the sector's growing reliance on data, digital platforms, third-party providers and connected technologies is expanding both the scale and speed at which risks can materialise.

For organisations operating in a highly visible, trust-dependent environment, even a single incident can quickly escalate into a multi-dimensional crisis affecting stakeholders, partners and public confidence.

HaysMac's Risk in Sport Pulse Survey explored how sports organisations are perceiving and responding to these evolving risks over the next 12–24 months. Drawing on responses from sports sector leaders, the findings reveal a sector that is alert to growing cyber and technology threats, but one that is still grappling with legacy systems, constrained resources and uneven board-level engagement — particularly when it comes to AI. Together, the results highlight a widening gap between awareness and readiness, suggesting that while risk is firmly on the agenda, governance structures and investment strategies are still catching up with the pace of technological change.

Key Findings

A converging risk landscape

The survey results show that cyber risk has become a defining feature of the sports risk agenda. 71% of respondents identified cybersecurity, cyber-attack or data breach as one of the most significant risks facing their organisation, making it the most frequently cited risk domain overall.

However, cyber risk rarely appears in isolation. 65% of respondents highlighted reputation and brand risk, underlining the extent to which a cyber incident is seen as a reputational event as much as a technical one. At the same time, 53% cited inflation and interest rates as a key concern, demonstrating that financial pressure continues to shape decision-making and risk tolerance across the sector.

Regulatory and compliance risk was identified by 41% of respondents, often in the context of data protection, AI usage and third-party oversight. While only 29% explicitly listed AI as a top risk, qualitative responses suggest that AI related exposure is embedded across cyber, compliance and reputational categories, rather than being viewed as a standalone issue.

Board engagement: progress, but not yet embedded

While awareness of technology and AI risk is growing, board engagement remains inconsistent. Only 24% of respondents stated that technology and AI risks are overseen "to a great extent" or are fully embedded at board level.

The majority (53%) described board engagement as moderate, suggesting that these risks are recognised but not yet deeply integrated into governance frameworks or strategic decision making.

A further 23% reported only limited board engagement, raising concerns that oversight may not be keeping pace with the scale and speed of technological change.

Several respondents pointed to a lack of strategic board focus or clarity of ownership, reinforcing the perception that technology and AI risk is still too often treated as an operational issue rather than an enterprise wide one.

Cyber readiness: confidence with caveats

Confidence in cyber incident preparedness is mixed: 59% of respondents rated their organisation's preparedness as high or very high, while 29% described it as moderate. However, 12% reported low or very low confidence, indicating a meaningful level of vulnerability within parts of the sector.

Importantly, even among organisations expressing higher confidence, there is an underlying concern that current controls may not be sufficient for future threats. Several respondents highlighted the rapid evolution of AI enabled cyberattacks, noting that organisations may be defending against today's threats without fully anticipating how attack methods are likely to develop.

What is holding organisations back?

When asked about the biggest barriers to improving resilience against technology, AI and cyber risk, respondents pointed overwhelmingly to structural constraints rather than lack of intent.

53% cited insufficient budget or resources as the primary barrier, reflecting the impact of wider financial pressures. 18% identified legacy or outdated IT systems, which limit the safe adoption of modern technologies and increase exposure to cyber risk. A further 18% highlighted limited understanding of the threat landscape, particularly at senior or board level.

Other barriers included unclear governance and accountability, regulatory uncertainty, and the challenge of operating in a continuously evolving technical environment where new gaps and risks emerge faster than controls can be implemented.

Where investment is increasing

Despite these challenges, organisations are actively investing to strengthen resilience. 65% of respondents expect to increase investment in cybersecurity tools, monitoring and threat detection, making this the most common area of increased spend.

Alongside this, 47% anticipate further investment in upgrading legacy systems and cloud migration, while the same proportion expect to increase spend on training, awareness and culture change. This reflects a growing recognition that technology alone is insufficient without corresponding investment in people and behaviours.

AI governance is also rising on the agenda, with 35% expecting increased investment in AI risk assurance, including model validation and explainability. Cyber and technology insurance and enhanced third-party risk oversight were also cited, signalling a more holistic approach to managing risk across the wider ecosystem.

Is sport more exposed than other sectors?

Perceptions of sector exposure are telling. 41% of respondents believe the sports sector is more exposed to cyber and technology risk than other industries, while 53% believe exposure is broadly similar. No respondents felt the sector was less exposed.

Those who viewed sport as more exposed pointed to high public visibility, valuable personal and commercial data, and complex third-party relationships as key drivers of risk. The combination of public scrutiny and digital dependence creates a risk profile that can magnify the impact of any technology failure or cyber incident.

The under-appreciated risks: AI and the extended ecosystem

One of the strongest themes emerging from the survey is the perception that certain AI related risks remain under appreciated at board level. Respondents highlighted AI enabled cyberattacks, deepfake technology, and data leakage through unprotected AI tool usage as growing threats.

Particularly notable was concern around third-party AI usage. Several respondents warned that suppliers with access to member, ticketing or financial data may already be using AI within their systems without sufficient transparency, governance or contractual clarity. This creates data protection, financial control and reputational risks that may not yet be fully reflected in risk registers or supplier oversight frameworks.

There was also a recurring theme around a lack of understanding of AI limitations, not just its opportunities, and the challenge of safely embedding AI into legacy systems.

Conclusion

The Risk in Sport Pulse Survey paints a picture of a sector at an important inflection point. Cyber risk is now firmly established as a core strategic concern, but AI related risks, particularly those arising from misuse, third parties and emerging technologies such as deepfakes, are still catching up in governance terms.

While investment is increasing and awareness is growing, the findings suggest that true resilience will depend on stronger board engagement, clearer accountability and a more forward-looking approach to technology and AI risk. For sports organisations operating in an increasingly digital and high-profile environment, the ability to anticipate and govern these risks may prove just as critical as on field performance.

How we can help

We help sports organisations strengthen governance, manage cyber and technology risk, and build resilient control environments through independent assurance and expert risk advisory. Our approach gives boards clarity, confidence, and practical actions to protect reputation and performance. Contact a member of the team to assess your risk exposure and take decisive steps to safeguard your organisation.

HaysMac Sports Team

Our specialists combine deep sector insight with technical expertise across risk, governance and technology, working closely with organisations to find practical solutions that stand up to real-world scrutiny. If you want to explore what they mean for your organisation, we'd welcome the conversation. It's what we're here for.

Tom Wilson

Partner, Head of Sport

twilson@haysmac.com

David Cox

Partner

dcox@haysmac.com

Dominic Noakes

Director

dnoakes@haysmac.com

Dougie Todd

Partner, Co-Head of VAT

dtodd@haysmac.com

Graeme Privett

Partner, Head of Private Client

gprivett@haysmac.com

Ian Cliffe

Partner

icliffe@haysmac.com

Nick Bustin

Director

nbustin@haysmac.com

Per-Olof Ahlstrom

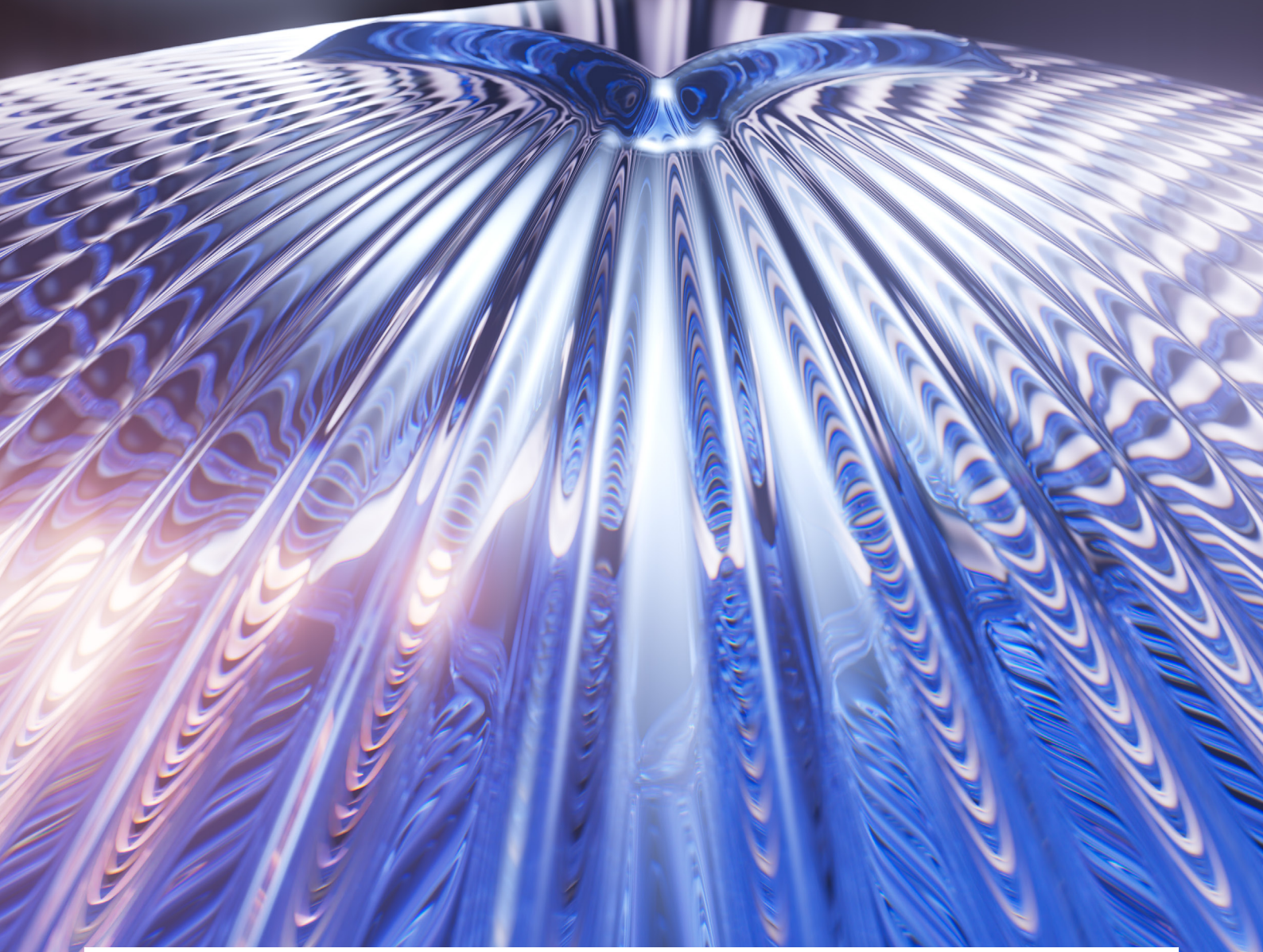
Director of Risk Assurance & Advisory Services

pahlstrom@haysmac.com

Sabina Burke

Partner

sburke@haysmac.com



HaysMac

A member of msi Global Alliance
Independent legal & accounting firms

We are a Living Wage Employer

Committed to Sustainability

10 Queen Street Place
London EC4R 1AG

T 020 7969 5500
E marketing@haysmac.com

haysmac.com

THE SUNDAY TIMES Best Places to Work 2025 BIG ORGANISATION

BRITISH BUSINESS EXCELLENCE AWARDS WINNERS 2025 LLOYDS

eprivateclient Top Accountancy Firms 2025

An eprivateclient top accountancy firm 2025