McLarens

Cyber risk and live events: a short window, high-impact exposure

Cyber risk is rarely out of the headlines. Attacks continue to increase in both frequency and sophistication. The NCSC's most recent Annual Review recorded 429 significant cyber incidents in the UK over a single 12-month period - more than double the figure from the year before, with 18 classified as "highly significant" in their potential to disrupt essential services. UK Government data shows that in 2024/25 the UK was the most cyber-attack targeted country in continental Europe.

In the entertainment and events sector, festivals, concerts, tours and corporate events operate within tightly defined timeframes, often supported by complex digital infrastructure. From ticketing platforms and access control systems to production networks, communications and payment processing, these events are increasingly reliant on interconnected technology. That dependency creates a distinctive risk profile: a short window of exposure, but with the potential for immediate and highly visible disruption.

With the summer events season approaching, what issues should be at the forefront of mind for insurers, brokers and policyholders in this sector?

A concentrated risk environment

The UK events industry is substantial. According to UKEVENTS, the sector contributed £61.65 billion to the UK economy in 2023. Business events alone - conferences, meetings, exhibitions and incentive travel - account for over £33 billion of that figure, with an estimated 1.08 million conferences and meetings taking place in 2024.

Unlike many traditional businesses, live events are inherently transient. A festival may run for days, a corporate launch for a single window. During that period and in the lead up, however, operations are intense and highly coordinated, and the financial consequences of disruption are immediate. The reliance on third-party ticketing platforms, payment processors and venue systems creates a dense supply chain where, as the NCSC has warned, a single compromise can cascade across multiple stakeholders. These pressures are already visible in the market: numerous festivals have been postponed or cancelled entirely for 2026, with rising insurance costs cited as a contributing factor.

The threat landscape

Ransomware, phishing and data exfiltration remain prevalent, while increasingly sophisticated attack models, including ransomware-as-a-service and multi-stage extortion, are becoming more common. Systemic risks are also growing. Incidents such as the CrowdStrike outage demonstrate that disruption need not stem from a targeted attack: a failure in a widely used platform can have immediate, global consequences.

For events, threats can range from attacks exploiting basic vulnerabilities, to targeted attacks seeking financial or personal data, to state-linked or ideologically motivated actors seeking to disrupt or discredit high-profile events. Internal risks are also a meaningful consideration: major events rely heavily on temporary contractors, making the internal risk harder to manage.

The regulatory horizon

The regulatory environment is also evolving. The EU's Cyber Resilience Act (CRA), progressively implemented since 2024, imposes mandatory cybersecurity requirements on manufacturers and suppliers of digital products – including networked light, sound, video and control systems standard in live event production – and requires suppliers and users to demonstrate compliance. In the UK, exact post-Brexit alignment remains unclear, but the draft Cyber Security and Resilience Bill proposes to extend similar obligations to the private industry, with implications for online ticketing, crowd management and event technical services. For cross-border touring and events, CRA compliance will be a practical necessity, and whether policy wording will reference legal compliance in this area is a question insurers and brokers will be considering.

Registration data and physical infrastructure

Attendee registration creates a concentration of personal data. For corporate conferences and industry summits, that concentration can be significant.

Physical infrastructure introduces further exposure. Venue WiFi, building management systems and networked access control are all potential attack vehicles. The NCSC recommends these systems be regularly patched (in accordance with vendors recommendations), tested and resilient to denial-of-service attacks, and advises that organisations running major events make contact beforehand to establish incident response protocols.

Insurance response and coverage challenges

Insurance solutions for cyber risk within events exist, but are often limited in scope and duration. Event-specific policies may cover only a defined number of days and specified geographic parameters. Cyber cover is frequently purchased as a policy extension rather than a standalone product, which creates gaps - business interruption cover, for example, may exclude certain cyber-related triggers.

Even where dedicated cyber policies are in place, limits can be quickly exhausted. For live events, where the financial impact of disruption is immediate and concentrated across ticket refunds, cancellation costs and reputational damage, the adequacy of existing cover warrants careful scrutiny.

Risk transfer versus risk management

As premiums rise and coverage becomes more restrictive, businesses are giving greater consideration to direct investment in cyber resilience: security software, real-time monitoring, staff training and managed security operations. For larger event operators, a more proactive approach to resilience may reduce both exposure and insurance cost over time.

That said, cyber incidents remain inherently unpredictable, and even well-protected organisations remain exposed, particularly to systemic risks and supply chain compromise outside their direct control.

Preparedness

The value of preparedness is a consistent theme in post-incident analysis. Scenario testing, clear communication protocols and predefined escalation pathways are essential.

Scenario testing for resilience to systems failure and cyber attacks should be planned and undertaken together with the implementation of robust business continuity plans (BCPs). Having cyber incident planning and procedures in place which are regularly reviewed can bring more awareness to the likelihood of a cyber attack and the procedures to be adopted should the worst happen.

With the weak link in the majority of cyber incidents being the human factor, regular staff training and cyber awareness is a key factor to preventing an incident or attack.

Pre-event penetration testing, access control management and keeping systems updated are practical steps that can significantly reduce both likelihood and impact. The human factor remains critical: in environments where large numbers of temporary staff cycle through quickly, training and awareness are harder to embed but no less important.

A developing risk

Cyber risk in live events is still evolving. While large-scale insured losses may not yet be widely visible, the underlying exposure is clear. The combination of digital dependency, compressed timelines and high public visibility creates a risk profile that is both distinctive and potentially severe.

Authors

Nigel Collins
Cyber, Technology
and Engineering Lead

+44 75 0311 9154
nigel.collins@mclarens.com

Ian McDonald
Head of Entertainment
and Contingency

+44 (0) 7970 884017
ian.mcdonald@mclarens.com