beazley

Article

When hackers take the field: Cyber risk and live events

Alexandra Sharps

A number of high-profile sporting events, festivals, fairs and concerts are taking place across the globe this summer, with millions of attendees set to descend on stadiums, amphitheatres, fairgrounds and parks with millions more tuning in elsewhere. Sporting events alone are valued at more than US$600 billion, with these events being the centrepieces of sporting and cultural calendars, and thereby prime targets for criminal cyber activity1.

From denial of access to disruptions in ticketing and other critical systems, the fallout from a cyber-attack can be severe. If major events are delayed or cancelled, the financial losses could run into the billions. Not to mention the cost later down the line should sensitive customer data be found to have been vulnerable and released.

Online opponents

As a sector, the events industry is particularly reliant on third party systems. For an event to take place as planned, every link in the chain needs to fulfil its role. From ticketing to transport, security to electricity, the event ecosystem is vast and, with every element increasingly digitally reliant, the opportunities for threat actors to gain access are myriad. The industry is not helped by the fact that there is no legal requirement for third party suppliers to hold any cyber security certification, and it is left up to the event organizer’s discretion.

Cyber criminals look for and target the weakest points in a system, with third party suppliers increasingly providing them with the entry point into larger organizations. Major events can also attract the attention of state-backed threat actors seeking to damage a host nation’s international standing. The scale of the problem was evidenced at the 2024 Paris Olympic Games, which experienced over 140 cyber-attack incidents2. Thankfully most were handled successfully and did not stop or delay the games – but this demonstrates the scale of the problem that event organizers face.

Perceptions of cyber risk among leaders in the hospitality, entertainment, and leisure sectors have remained steady, according to our latest Risk & Resilience research data3, with **26%** ranking it as their top concern - unchanged from 2024. This contrasts with the global trend, where concern has risen with **29%** of leaders now cite cyber risk as their top issue, up from **26%** the previous year.

Does this point to an underestimation of the threat? And with **81%** of leaders in the sector reporting confidence in their cyber preparedness - could they, in fact, be overestimating their resilience?

Getting event ready

Our claims data indicates the continued need for comprehensive protection to counter cyber risk. A full spectrum approach, where organizers pre-emptively prepare for cyber-attacks, to enable them to respond quickly and appropriately to an attack and continually adapt their cyber defences as the risks evolve, is needed as part of a wider event cancellation strategy.

Additionally, event cancellation insurance policies are rarely extended beyond insureds' and contracted parties' computer system breakdowns, excluding malicious intervention, leaving events financially exposed to potential cancellation from a cyber-attack.

An insurance solution should be an integral component of a wider mitigation strategy. Many market offerings and cyber responses are fixed to the event and focused on insureds' and contracted parties' non-malicious computer system failures or the impact on attendees. Yet, this leaves gaps in cover.

The ideal policy is tailored to counter cyber threats in a comprehensive and robust approach, offering protection for a wide range of scenarios. The right cover for an event will not only support organizers with the response to a cyber-attack, protecting event companies from the repercussions of cancellations or abandonments triggered by cyber disruptions, but also offer pre-emptive risk management advice, building resiliency in the face of the evolving cyber risk.

Alexandra Sharps

Product Leader - US Contingency

[1] https://www.microsoft.com/en-us/security/security-insider/intelligence-reports/cyber-signals-issue-5-cyberthreats-increasingly-target-the-worlds-biggest-event-stages/

[2] France reports over 140 cyberattacks linked to Olympics

[3] Methodology | beazley

beazley