beazley

Article

Major sporting events at the mercy of cyber criminals

Andrew Duxbury • September 10, 2024

A number of high-profile sporting events are taking place across Europe this summer, with millions of fans set to descend on stadiums and billions expected to tune in across the globe. These events are the centrepieces of sporting and cultural calendars. Billions could be lost if they are delayed or cancelled.

Cyber criminals target organisations where they can exert leverage or simply cause wanton disruption. While attacks can drive a loss of revenue from denial of access to systems and compromise sensitive customer information, cyber criminals know that once an event is cancelled, they are unlikely to extract any payments. By this point, there is likely to be no further leverage.

With the eyes of the world watching, the pressure which these events can potentially exert on organisers is immense and cyber threat actors have taken note. The UK's National Cyber Security Centre (NCSC) found that cyberattacks against sports organiszations are increasingly common, with 70 per cent experiencing at least one attack per year[1].

Rising cyber threat for event organisers

Leverage is just one reason why cyber criminals are targeting the events industry. As a sector, it is also 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 are **no legal requirements** for third party suppliers to hold any cybersecurity certification as it is left up to the event organiser's discretion.

Hackers look for and target the weakest points in a system, with third

party suppliers increasingly providing them with the entry point into larger organisations. Major events can also attract the attention of state-backed threat actors seeking to damage a host nation's international standing. The infamous 'Olympic Destroyer' malware targeted Pyeongchang's opening ceremony at the 2018 Winter Games causing widespread concern. The hackers infiltrated internet and television services meaning tickets couldn't be printed resulting in an unusually high nonattendance and WIFI used by media reporting the games didn't work.

Business leaders recognise the threat. Our latest Risk & Resilience data shows that over a quarter (26%) of business leaders in the hospitality, entertainment and leisure industry cited cyber as the biggest threat they face this year. This is set to rise to 30% by 2025.

Getting event ready

Against the backdrop of this rising threat, the need for comprehensive protection to counter cyber risk is clear. A full spectrum approach, where organisers pre-emptively prepare for cyber-attacks, respond nimbly to hacks and continually adapt their cyber defences, is needed as part of a wider event cancellation strategy. However, contingency 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.

If hackers do gain entry, it is important to have multiple layers of defence in place to prevent the worst outcomes. Our data finds that a quarter (25%) of business leaders in the hospitality, entertainment and leisure industry feel unprepared to counter the threat posed by cyber risk this year.

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.

The ideal policy tailored to counter cyber threats is comprehensive and robust, offering protection for a wide range of scenarios. The right cover can support with the response to a cyber-attack, protecting events from the repercussions of cancellations or abandonments triggered by cyber disruptions. Insurers providing this cover must combine contingency and cyber knowledge to deliver a comprehensive solution.

Andrew Duxbury

Head of Contingency

BZPAC218.

[1]https://www.ncsc.gov.uk/files/Cyber-threat-to-sports-organisations.pdf

beazley