Aon
Cyber Solutions

Sport & Entertainment

Cyber risk exposures and solutions

Hospitality organisations such as hotels, event promotions, theme parks and tourism agencies are a target for cyber criminals with motives of financial gain via theft of confidential information or money. Cyber is a broad risk that organisations face by virtue of their reliance on information technology, connectivity and automated processes. In an increasingly punitive legal and regulatory environment, and with more frequent contractual requirements for cyber liability insurance, forward thinking companies are taking proactive steps to explore and transfer cyber risk.

Numerous factors contribute to an organisation's cyber risk profile, including: action by employees, system and programme errors, security measures, industry, nature and quantity of data collected, political or strategic significance and reliance on technology.

Cyber risk considerations for sport and entertainment organisations:

- Gathering, maintaining, disseminating or storage of private information
- Hackers targeting Point-of-Sale systems (POS) or third party vendors to gain access to the organisation's network
- Privacy regulation
- High dependency on electronic processes and computer networks
- Third parties (including payment processors) and fourth parties (specialist firms who oversee outsourced service providers)

Potential cyber incidents for sport and entertainment organisations:

- Unauthorised access to online ticket sales / booking systems
- Malware installed on POS terminals at front desks
- Exposed credit card data of customers
- Social engineering
- Exposed credit card information
- Intentional acts committed by rogue employees
- Ransomware attacks

We're here to empower results

Alistair Clarke
Cyber Sport & Entertainment Industry Expert
+44 (0) 20 7086 7357
alistair.clarke@aon.co.uk

Shannan Fort
Cyber Insurance Leader
Global Broking Centre
+44 (0)20 7086 7135
shannan.fort@aon.com

David Molony
Cyber Risk Leader
Global Risk Consulting
+44 (0)777 5227008
david.molony@aon.co.uk

Spencer Lynch
Cybersecurity Leader
Stroz Friedberg
+44 (0)20 7061 2304
slynch@strozfriedberg.co.uk

Vanessa Leemans
Chief Commercial Officer
Cyber Solutions EMEA
+44 (0)20 7086 4465
vanessa.leemans@aon.co.uk

aon.com/cyber
strozfriedberg.com/resource-center

Empower Results®

Scope of traditional cyber coverage available in the insurance marketplace:

Third party coverage elements

- ***Security and privacy:*** defence costs and damages suffered by others resulting from a failure of computer security, including liability caused by theft or wrongful disclosure of confidential information, unauthorised access, denial of service attack or transmission of a computer virus
- ***Regulatory defence and fines:*** defence costs for proceedings brought by a governmental agency in connection with a failure to protect private information and / or a failure of network security
- ***Media liability:*** defence costs and damages suffered by others for content-based injuries such as libel, slander, defamation, copyright infringement, trademark infringement, or invasion of privacy
- ***PCI fines and assessments:*** defence costs for investigations brought by the Payment Card Industry (PCI) in connection with a failure to protect private information and / or network security

First party coverage elements

- ***Breach response costs associated with:*** breach notification, including the hiring of outside law firms and public relations consultants, forensic costs, credit monitoring / protection, notification hot-line / call centre, identity theft resources
- ***Network business interruption:*** loss of income and extra expense due to network security failure
- ***Dependent business interruption:*** reimburses the insured for actual lost net income and extra expense incurred when the insured's service provider's computer system is interrupted / suspended due to a failure of network security
- ***System failure business interruption:*** coverage for business interruption due to an unintentional or unplanned system failure not caused by a failure of network security
- ***Data restoration:*** costs to restore / recreate data / software resulting from network security failure
- ***Cyber extortion:*** reimburses the insured for expenses incurred in the investigation of a threat and any extortion payments made to prevent or resolve the threat

Aon has successfully negotiated the following key coverage enhancements (subject to market agreement per individual risk):

- Full limits for incident response and costs associated with breach notification
- Broad definition of computer system
- Coverage for cyber terrorism
- Deletion of the unencrypted device exclusion
- No failure to patch exclusion

Empower Results®

Our approach

Adopting a risk based cyber insurance strategy

Aon's cyber capabilities can support organisations in embracing a risk based approach through:

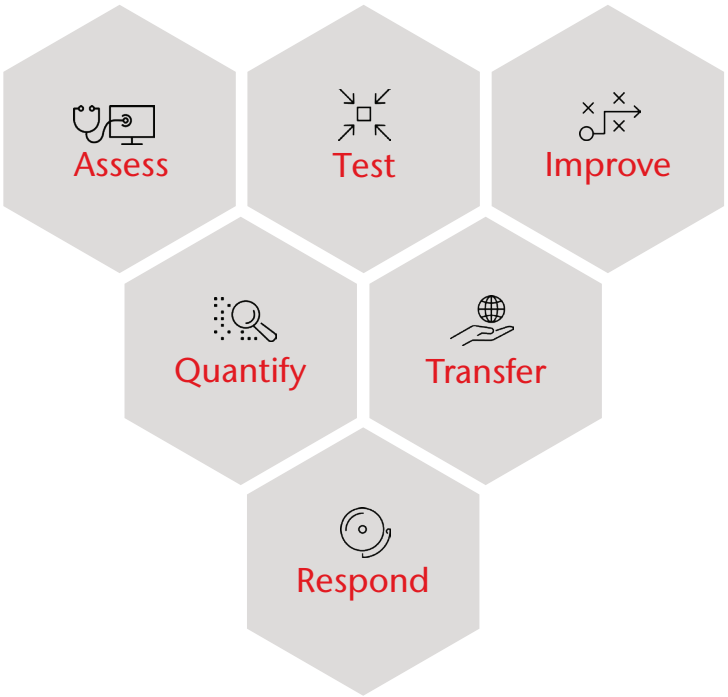
- *Cyber Assessment* - an enterprise wide approach to cyber security risk that provides a detailed view into an organisation's unique technology profile and threat landscape, with a focus on facilitating risk quantification and insurability.
- *Cyber Impact Analysis* - a data driven analytical framework supporting organsations to optimise their resilience strategy through mitigation and transfer. Existing risk financing strategies can also be enhanced through modelling cyber loss scenarios and stress testing current limits.

Cyber innovation

- *Aon Cyber Enterprise Solution*™ - a policy which broadens the scope of cyber coverage to include: property damage arising out of a network security breach, business interruption and extra expense coverage arising out of a systems failure, contingent network business interruption for IT vendors and the supply chain, cyber terrorism coverage, etc.
- *Aon's GDPR Protect Solution* - a modular risk management solution that helps organisations manage financial, regulatory and legal risks associated with processing personal data under the EU General Data Protection Regulation (GDPR).

Our cyber resilience framework

Aon and Stroz Friedberg offer a full range of services to help you approach cyber as an enterprise risk and achieve cyber resilience.



Empower Results®

Client story

A professional sports club was faced with a sensitive personnel situation when they sought to terminate the employment of a senior IT staff member. The decision to terminate was not in response to performance issues or any wrongdoing. Instead, the individual was not seen as the best fit for the future direction of the club, making the situation even more delicate. Senior executives and head of security of the club realised that the termination posed a potentially serious insider risk given that a technically adept person with the employee's profile could either sabotage the computer network environment or craft a back door, allowing remote access after departure to gain unauthorised network access. Aon was hired to perform an insider cyber risk assessment.

Our technical experts at Stroz Friedberg assessed existing vulnerabilities and provided recommendations for technical steps that could be taken to mitigate the threats posed by the departing insider. In addition, our behavioural science experts advised the club on best practices for how to handle the termination notification and the exit interview, and how to maintain contact with the individual post-employment to monitor behaviour and gather useful feedback.

By creating multidisciplinary teams that combine human intelligence with science and logic, we provided a holistic approach to mitigating the organisation's insider risk. The club adopted our recommendations, and the transition of the employee went smoothly with no adverse consequences.