Cyber risk in the active leisure sector

If you think cyber risk isn't something you need to worry about, think again!

From climbing wall centres, bungee runs and high ropes, to soft play, inflatable parks and escape rooms – the threat of cyber crime and its impact on the active leisure sector is now a real concern.

What is Cyber Risk?

Cyber risk is one of the most talked about topics in business and the media. Advances in technology have provided unparalleled levels of convenience in our business and personal lives but have also increased our exposure to the new risk of cybercrime. From ransomware and hacking, to identity theft, extortion and electronic fraud – businesses now face financial loss, litigation and reputational damage due to this new form of online criminal activity.

What if?

- Your data security measures fail and customers' personal information is breached?
- The booking system you depend upon is hacked and your customers can no longer book online or access their data online?
- The payment card system you use is compromised and funds are stolen?
- The data regulator decides to investigate you following a data breach?
- You're locked out of your computer network in a malware attack and the cyber criminal demands a ransom?

Why is Active Leisure a target?

- Leisure firms hold personal information on customers, staff and members. This data is attractive to cyber criminals who can use it to perform different types of online criminal activity.
- Theft or breach of data (including payment card information) can lead to costly liabilities and regulatory investigations.
- Organisations in this sector often rely upon third party software providers, such as membership management systems, booking & billing apps and automated marketing services.
- An attack on these systems could lead to downtime, disgruntled customers and lost revenue.

How big is the problem?

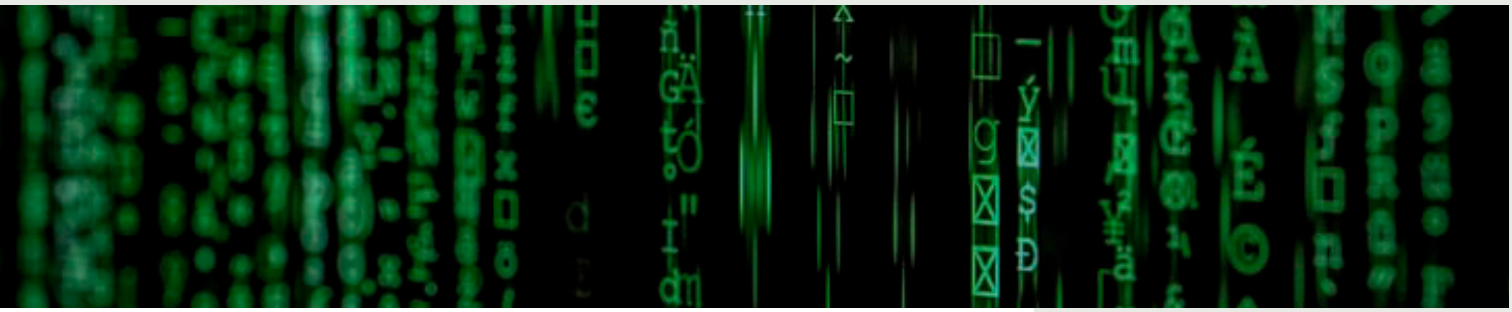
In its 2022 Cyber Security Breaches Survey, the government found that 39% of UK businesses have identified at least one cyber-attack in the past 12 months.

In its 2022 Cyber Readiness Report, Hiscox found that one-in-five firms attacked say their solvency was threatened, an increase of 24% from last year. The median cost of an attack in the UK is now £23,600.

In the same report, Hiscox found that small and mid-size businesses are bearing the brunt – firms with revenues of up to £350,000 now get as many attacks as those with revenues of up to £7.5m.

A poll released by Allianz in 2022 revealed that cyber incidents have become the most important business risk.

Cyber risk in the active leisure sector



What can be done to reduce the chance of a cyber-attack?
Some practical steps can help mitigate the risks:

- Staff training – turn your staff into your first line of defence by training them how to recognize common types of cyber-attack, such as email phishing attacks.
- Back-up your data – it's a good idea to maintain regular back-ups, segregated from your main network.
- Use multi-factor authentication – ensure MFA is enabled for all remote access to your network.
- Patch & Update – use only software that's supported and regularly updated, to ensure any vulnerabilities are 'patched'.
- Protect mail – ensure email filtering software is enabled.
- Plan for a crisis – to ensure you know what to do if the worst happens.
- Insure – cyber insurance is the ultimate backstop and can protect you against liability for downtime, privacy liability, regulatory investigation, fines & penalties, lost profit, additional costs, brand damage and breach expenses.

Matthew Clark
CYBER DIRECTOR

+44 (0) 7775 537 387
matthew.clark@partnersand.com

MATTHEW CLARK

Partners&

m +44 (0) 7775 537 387
e matthew.clark@partnersand.com
w partnersand.com

Connect with us on:

Investor in Customers® Gold 2021