Case Study

ASTONLARK

The insured	Golf Club
Revenue	£3.5m
The sector	Leisure
The incident	The club suffered from a ransomware attack that froze its entire server. This included the point of sales registers for the golf operations and the club restaurant. The hacker had demanded c.£18,000 in Bitcoin to decrypt and release the systems. The insured was unable to retrieve or access their backups.
The trigger	Breach costs, Privacy Liability, Business Interruption, Ransom costs
Threat factor	Ransomware
The result	Hiscox instructed forensics to establish if any data had been harvested by the ransomware or by the hacker. Furthermore, Hiscox paid the ransom after determining the threat to be genuine and the decryption key provided by the hacker would in fact release the server. Throughout this process, Hiscox liaised with legal counsel to determine potential breach obligations and advise on all investigations. The club's operations were restored and counsel concluded there were no data notification obligations.
The cost	£22,000
The takeaway	The insured was swift to notify Hiscox, which meant no significant loss of revenue occurred. In addition, customers can make use of Hiscox CyberClear Academy, which provides e-training to help our customers' staff to spot malicious emails containing ransomware.
Premium	**£5,000**

www.astonlark.com/cyber

020 8633 8430