Case Study

ASTONLARK

The insured	Personal Training Firm
Revenue	£8m
The sector	Coaching, Learning & Education
The incident	An employee received an email from someone purporting to be the CEO, requesting a wire transfer to a retail bank account. The employee prepared and released the payment the same day. A few days later, a second request was made and it was then the fraudulent activity of the previous day was uncovered.
The trigger	Cyber Crime, Privacy Liability
Threat factor	Social Engineering
The result	Hiscox paid the amount that was transferred to the fraudulent account. In addition, Hiscox instructed forensics and legal breach coaches to determine if this event was caused due to a network breach. It concluded no breach had occurred and the loss was a direct social engineering event from a criminal third party email
The cost	£24,000
The takeaway	Along with insurance protection, it is always wise for companies to impose dual authentication for any fund transfers and to improve security awareness of all employees with training to help them spot spear fishing emails of this kind.
Premium	**£5,000**

www.astonlark.com/cyber

020 8633 8430

Chartered Insurance Brokers

AL-COM-004-0220