Case Study

ASTONLARK

The insured	HVAC Product Distributor
Revenue	£390m
The sector	Manufacturing
The incident	The insured provides distribution services for HVAC equipment, both online and at brick and mortar locations. Ransomware infected the insured's servers, encrypting all files and causing a shutdown of the retail website and loss of access to key systems at the physical locations. The insured did not pay the ransom and recovered from back-up. Within four days, the insured's systems were restored and functioning, and its facilities were open for business on a partial resumption schedule.
The trigger	Breach Costs, Business Interruption
Threat factor	Ransomware
The result	Hiscox instructed specialist privacy lawyers to advise on regulatory notification obligations to those affected. Meanwhile, a call centre was set up on behalf of the insured to help those affected after they were notified of the incident. Credit monitoring services were then implemented to check none of the data subjects details were being circulated publically for fraudulent means.
The cost	£563,532
The takeaway	Along with insurance protection, a tested backup strategy is essential in protecting businesses from ransomware attacks and mitigating business interruption. A company of this size should be utilising both regular connected backups and disconnected backups to mitigate the risk of their cloud backups also getting encrypted.

Premium	**£10,000-£20,000**

www.astonlark.com/cyber

020 8633 8430