Cyber Insurance

A case study

ALAN BOSWELL
Insurance Brokers

Ransomware - denial of service attack | High Street Retailer | Claim in excess of £1 million

The policyholder is a retailer with over 100 stores.

Whilst they were undertaking some changes to their IT storage they suffered a sophisticated cyber attack which encrypted all their files, including those held in the cloud. The attackers demanded a ransom for providing a 'decryption code'.

The shops were still able to trade using manual tills but the attack left them unable to replenish stock in stores and process online orders which led to a major business interruption.

The policyholder held a full cyber package and used the following heads of cover:

Cyber extortion

After a prolonged period of being unable to fully trade the decision was taken to pay the ransom which was $150,000. This particular policy gave provision for paying the ransom but whether this course of action was taken or not was at the policyholder's discretion. Insurers had to use specialist suppliers to source bitcoins.

Event Management

Fees and costs associated with managing the attack, mostly legal costs and PR.

Network interruption

Forensic IT specialists were appointed by insurers within 24 hours and were on site non-stop for long periods. Initially securing the system and trying to see if any data could be retrieved. After the ransom was paid the decryption code was provided but all files had to be manually decrypted using the code which was a painstaking and costly process in terms of labour.

The insured also had to pay additional fees to their various existing software providers for additional support and equipment.

Cyber liability

On this occasion there was no evidence any customer data was held or extracted so no action was required by the ICO but the insured required legal & IT advice to determine this.

Business interruption

This makes up a large proportion of the claim and is perhaps the most undervalued area of cover. Even having paid a ransom, trading was still majorly impacted and the policy limit was breached as a result.

Directors' & Officers'

This customer's D&O cover had a cyber extortion extension which was a contingent cover, this has assisted with costs not met by the cyber insurer either by way of exclusion or because the limit has been exhausted. This incident was also noted as a material fact as trading was impacted and Directors were making business critical decisions. The company had a history of shareholder disputes.

Whilst this attack appeared to be targeted most ransomware attacks are generated by software that are directed en-mass usually by way of phishing emails which unwitting staff open. Even if customers are benefitting from the cloud or not storing customer data how would their trading be affected and could they afford the fees of experts whilst managing a breach. Costs alone on this case will likely exceed £300K.