

OUR INSURANCE IN ACTION

We have dealt successfully with many cyber and data related claims. From a client held to ransom by a Russian hacker, to a customer being tipped-off by 'white hat hackers' that their information was for sale on the dark web, here are some recent examples.

The technology business and malware

Cost covered by Hiscox: £250k



Our client was contacted by a government agency and advised that government security services had detected an intrusion on its systems. Our IT forensic experts were deployed to investigate and assess the extent to which the network had been compromised. A significant amount of malware was discovered on our client's servers so a containment plan was executed to remove all malware. Our client was also able to take legal and PR advice under their insurance cover to help them decide how and when to communicate this incident to their clients.

The optician held to ransom

Cost covered by Hiscox: £60k



An employee from a chain of opticians – received an email to say that she had been caught speeding and clicked the button which offered to show a photograph of her being caught in the act. Shortly afterwards our client received an email from someone in Russia to say that they had infected their systems with the Cryptolocker virus and that all files on its servers were encrypted. The encrypted files included patient records and software used to run the business. The Russians were asking for £400 in Bitcoins for the decryption key. We approved the client's payment of the ransom. Unfortunately this only recovered 90% of the files and they needed an IT contractor to help them recover the remainder. Their insurance policy covered this business interruption as well as the costs of being unable to trade for a couple of days and not being fully up-to-speed for a couple of weeks.

The publisher's lost passwords

Cost covered by Hiscox: £10k



Contacted by a 'white hat hacker', our client was told that user names and passwords for two of their websites had been stolen. We called in IT forensic experts to investigate, who confirmed there had been a hack and set about plugging the security breach. Legal advice was also taken to confirm whether or not our client was required to notify the individuals whose user names had been compromised.