

# Cyber Liability Insurance - FactSheet

## Cyber Liability Insurance - Protecting your intellectual property online

Online exploitation of intellectual property is rising according to new study

The UK is in the grips of a cybercrime wave with many businesses unaware of how their

brand is being used online following the release of a report investigating the serious issue of 'brand jacking'.

The latest Brand jacking Index demonstrated an increase in the number of businesses falling prey to incidences of 'brand jacking' – when a third party registers a domain name that infringes upon or otherwise violates the rights of a trademark owner.

With many businesses unaware as to how to protect their Intellectual Property (IP) online, cybercriminals are able to buy relevant domain names and abuse the brand image for their own gain. Macbeth is asking businesses to review the value of their brand online and evaluate what cover they have to pursue those who infringe their IP rights?

Your brand is your good name, it is the embodiment of your reputation and drives business to your door, so any misuse of your brand online could have significant financial consequences. Yet, very few organisations make any attempt to protect themselves from such financial loss.

Each week, nearly 3500 domains are hijacked from rightful owners, any business could easily fall victim to brand and domain theft, which if left unchecked, can seriously impact the value of its trademark, as well its bottom line.

2008 saw significant rises in the incidences of cybercrime including 'cyber squatting' (registering a brand based domain name with the aim of selling it on to the brand owners at a profit) which rose by 18% and false association (registering a domain name similar to an existing brand in order to misdirect users who have typed a website address wrongly).

The Brand jacking Index states 440,584 instances of cyber squatting were identified in the fourth quarter of 2008 and 86,837 instances of false association. However, no less than 80 percent of the websites identified as fraudulent or abusive in 2007 were still online in 2008 with the majority of these hosted in the UK, the US and Germany.

Incidences of 'phishing' (sending bogus emails designed to mislead recipients into revealing passwords, credit card numbers and other sensitive information) are also increasing.

If an individual is successfully 'phished', they may be duped into divulging sensitive details such as passwords and bank account details. The same is true for businesses, however the consequences can be more severe with not only an organisation's sensitive information accidentally divulged, but also that of its customers. If a company is not actively working to protect its customers' private information, it will be liable to prosecution.

As the Internet has transformed into a central component of daily life, so online brand fraud and abuse has grown steadily, devaluing IP, damaging hard-earned reputations and eating into profits. But those companies that take a proactive approach to protecting their assets and digital liabilities are those which are most successful in responding to this threat.

For more information on internet liability and cyber liability insurance, please contact Tony Gibbs on 0118 9452944.

