

CONFERENCE FEATURE

Lawful intercept

Sales director of guest internet provider Airangel Dean Wilkinson warns that new Lawful Intercept legislation in force since March brings serious implications for the conference industry.

Wi-Fi provision is now widely accepted as a vital service among conference venues, hoteliers and others in the events industry. Increased interest in social networking sites and the emerging 24/7 working culture which Blackberries and other PDAs have brought about, have made Wi-Fi an important and often lucrative service offering. But do you know who's making use of your Wi-Fi services?

For the most part no, but as of 15 March new legislation demands that if you offer Wi-Fi services you should know who's using them and what they're looking at.

Called Lawful Intercept, the directive means that you must keep records of all the communications that take place over your venue's internet connection and attempt to identify and record the user. For conference venues and organisers, this means retaining the information of all communications made by delegates.

The directive is a response to the heightened use of the internet in organised crimes such as data theft, paedophilia and, in particular, terrorism, and is designed to reduce the associated risks for society as a whole. The required information must be collected, stored and made available for authorities to access at any time including the police, health authorities, council and government.

Whose responsibility is it?

So why isn't it enough that your internet



Wilkinson: 'Do you know who's making use of your Wi-Fi services?'

service provider (ISP) collects and stores this information on your behalf? In truth, this just doesn't afford you enough protection and while the penalties of not complying aren't yet known, the potential risks to your brand reputation and image make it an issue that can't be ignored.

Take for example a haulage company. If a haulier's lorry was caught speeding on the motorway, it wouldn't be the company that would be liable for a fine or penalty, it would be the driver of that lorry. The management would be able to identify the driver of that particular lorry by checking their records to see who had what lorry on what day.

The same thinking applies to your business under the Lawful Intercept directive. If a haulage company will pass the authorities onto the speeding driver, so too will ISPs to your business.

In real terms, this means that your business is responsible for knowing who accesses the internet or emails via your server and requires you to store information on user IDs, IP addresses and the date and time of communication. They should be able to trace the source of communications, times and locations of equipment and the nature of the communication. This information has to be stored for up to two years.

How do I protect my business?

There are some straightforward steps which can be implemented quite readily. Firstly, in addition to speaking with your ISP you should seek advice from your other IT partners, be they IT help desks or Wi-Fi and guest internet access providers.

These companies can ensure your system is Lawful Intercept compliant as part of their service and take the hassle out of the process for your business and your staff. Make sure you get comprehensive advice and find the best solution to fit your needs.

Other suggestions include linking delegate registration and other data-capture systems to your tracking logs to ensure compliance. By making sure you capture as much information about your delegates' identities when they register or log on to your internet network, you are going some way to meeting these obligations.

Critics of the legislation argue that the validity of this information is questionable as those engaged in criminal activities will use false identities to evade detection. However, while this may be true, those operating in the events industry have an obligation to comply and a duty to protect their brands and reputations.

Contact Airangel at www.airangel.com or T. 08707 667 516